Information Friction:
Information Technology and Military Performance

by

Jon Randall Lindsay

B.S. Symbolic Systems
Stanford University, 1995

M.S. Computer Science
Stanford University, 1997

SUBMITTED TO THE DEPARTMENT OF POLITICAL SCIENCE IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY IN POLITICAL SCIENCE
AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

FEBRUARY 2011

Signature of Author: _____
Department of Political Science
January 28, 2011

Certified by: _____
Barry R. Posen
Professor of Political Science
Dissertation Adviser

Accepted by: _____
Roger D. Petersen
Professor of Political Science
Chairman, Graduate Program Committee

Information Friction:
Information Technology and Military Performance

by

Jon R. Lindsay

Submitted to the Department of Political Science on January 28, 2011 in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Political Science

ABSTRACT

Militaries have long been eager to adopt the latest technology (IT) in a quest to improve knowledge of and control over the battlefield. At the same time, uncertainty and confusion have remained prominent in actual experience of war. IT usage sometimes improves knowledge, but it sometimes contributes to tactical blunders and misplaced hubris. As militaries invest intensively in IT, they also tend to develop larger headquarters staffs, depend more heavily on planning and intelligence, and employ a larger percentage of personnel in knowledge work rather than physical combat. Both optimists and pessimists about the so-called "revolution in military affairs" have tended to overlook the ways in which IT is profoundly and ambiguously embedded in everyday organizational life. Technocrats embrace IT to "lift the fog of war," but IT often becomes a source of breakdowns, misperception, and politicization.

To describe the conditions under which IT usage improves or degrades organizational performance, this dissertation develops the notion of *information friction*, an aggregate measure of the intensity of organizational struggle to coordinate IT with the operational environment. It articulates hypotheses about how the structure of the external battlefield, internal bureaucratic politics, and patterns of human-computer interaction can either exacerbate or relieve friction, which thus degrades or improves performance. Technological determinism alone cannot account for the increasing complexity and variable performances of information phenomena.

Information friction theory is empirically grounded in a participant-observation study of U.S. special operations in Iraq from 2007 to 2008. To test the external validity of insights gained through fieldwork in Iraq, an historical study of the 1940 Battle of Britain examines IT usage in a totally different structural, organizational, and technological context. These paired cases show that high information friction, and thus degraded performance, can arise with sophisticated IT, while lower friction and impressive performance can occur with far less sophisticated networks. The social context, not just the quality of technology, makes all the difference. Many shorter examples from recent military history are included to illustrate concepts. This project should be of broad interest to students of organizational knowledge, IT, and military effectiveness.

Thesis Supervisor: Barry R. Posen
Title: Ford International Professor of Political Science

Table of Contents

Biographical Sketch

Jon Lindsay hails from San Diego, California. From Stanford University he received a B.S. degree in Symbolic Systems (an interdisciplinary program in philosophy, psychology, linguistics, and computer science) and an M.S. degree in Computer Science, specializing in human-computer interface design.

He was commissioned an intelligence officer in the U.S. Navy and served as a targeting analyst at the Naval Strike and Air Warfare Center ("TOPGUN"), targeting officer with Joint Task Force Noble Anvil during Operation Allied Force (Kosovo, 1999), intelligence officer of Naval Special Warfare Unit Four under Special Operations Command South, and member of the Naval Special Warfare Mission Support Center during Operation Iraqi Freedom (2003). In the Naval Reserve while at MIT, he supported the Chief of Naval Operations Strategic Studies Group, provided Office of Naval Intelligence liaison to Lawrence Livermore National Laboratory on high-performance computing support to analysis, and mobilized to active duty to serve as Officer in Charge of Tactical Intelligence Support Team Four and Non-Lethal Effects Officer of Special Operations Task Force West (Iraq, 2007-2008).

As a graduate student in the MIT Department of Political Science, he was a member of the Security Studies Program and the Program on Emerging Technology (PoET). His research and teaching interests span international security, the sociology of science and technology, information science, and irregular war. He has published in the journal *Technology and Culture*, contributed chapters to edited volumes, and has consulted for various public and private organizations on defense-related topics. After completing this dissertation at MIT, he took a postdoctoral position with the University of California Institute on Global Conflict and Cooperation, Project on the Study of Innovation and Technology in China, located at the University of California, San Diego. He can now be found enjoying seventy-degree winters and the perfect granite of the Sierra Nevada.

Figure 0-1: The Military Meets MIT (Author's photo)

Acknowledgements

In my application to MIT eight years ago I asked "what can cognitive and information science tell us about how Leviathan knows?" This question has received refinements and new directions aplenty since then, but clearly there are some threads that link undergraduate interests in the philosophy of mind, experiences in the Navy with war and bureaucracy, and this latest interdisciplinary effort. This project has been a long time in coming, and I have incurred many debts along the way.

My dissertation committee generously provided their time and feedback on my inchoate drafts. Barry Posen continually pushed me to temper my attraction toward complexity to get to the essence of the matter. Ken Oye's mentorship in the political economy of technology and material assistance for research has been invaluable. Wanda Orlikowski reassured me about the value of interdisciplinary work and gave me a crash course on ethnography. I am indebted to Merrit Roe Smith for introducing me to the history of technology and for his example of careful scholarship. Many other scholars have offered support and inspiration along the way: Roger Petersen, Owen Coté, Jr., Stephen van Evera, Eric von Hippel, Harvey Sapolsky, David Clark, Piet Hut, Nazli Choucri, Jack Goldsmith, Terry Winograd, Peter Godfrey-Smith, and René Girard. Essential intellectual, material, and administrative support was provided by the MIT Political Science Department, MIT Center for International Studies, MIT Program on Emerging Technologies (a National Science Foundation Integrative Graduate Education Research and Traineeship), and the Office of Naval Research under award number N00014091059.

The conversations, examples, and camaraderie of my peers have truly been the highlights of graduate school. Hanna Breetz, Kieran Downes, Ben Friedman, Brendan Green, Phil Haun, Llewelyn Hughes, Shirley Hung, Colin Jackson, Austin Long, Will Norris, Andrew Radin, Josh Rovner, Gustavo Setrini, Josh Shifrinson, Paul Staniland, and Caitlin Talmadge: good friends in discovery and common suffering make graduate school not only endurable but occasionally enjoyable. Other friends enabled various adventures, vertical and otherwise, to cheer my New England exile: Karen Cruz, Nicole Davis, Allan Friedman, Aaron McMillan, Heather Silverberg, Amy Sun, and Edita Zlatic. Thanks also to the Boston Red Sox for the 2004 season and for making this a really fun town to call home. All gave me reason to temper academic hermitage and LTHOADACH: Leave The House Once A Day And Contact Humans.

I am grateful to the U.S. Navy for comrades, intellectual stimulation, and fieldwork opportunities. Michael Perkinson originally inspired my interest in international relations and has always offered wise counsel. I've benefitted tremendously over the years from Paul Harris Wilt's intelligence, insight and generosity, not to mention a little Access database called *Quiver*. Mary Ann Dorsey encouraged me to just keep swimming! John Robinson, Jeff Cadman, and Scott Douglas gave their time to read drafts of chapters and helped me to survive the reserves with humor in tact. Many other officers provided assistance and encouragement: Jim Ford, Ken Elkern, Pete Oswald, Tom Brown, Pete Wikul, John Jacobs, Dane Thorliefson, Chris Connor, Paul Hastert, and John Chilton. I would especially like to thank the men and women of Tactical Intelligence Support Team Four and SEAL Team One for the honor of serving alongside them. The opinions, findings, conclusions and recommendations expressed in this project are mine alone, of course, and do not necessarily reflect the views of the Navy or any other organization.

Finally I would like to thank my family for their love and understanding during these long years. They endured many quizical looks from friends who asked what I was up to when I was unable to articulate it very well myself. My parents, Lowell and Diana Lindsay, have been endless sources of energy, humor, intellectual inspiration, and affection. My sister Jenn Lindsay provided music, confidence, and family while we were both too far away from that great spiritual battery which is California. Carrie Lee saw me through the tumultuous final stretch of this project and gave me much to look forward to in future journeys. I couldn't ask for more.

Heartfelt thanks to all those mentioned here and to those I have been unable to include. This project is better for their influence. Its many flaws remain my own responsibility.

List of Tables

List of Figures

Chapter 1: Introduction

"We know more, but this makes us more, not less uncertain."
– Carl von Clausewitz[1]

1.1 Has the Information Revolution Improved Military Performance?

Conventional wisdom holds that information technology (IT) has fostered a "revolution in military affairs" (RMA). RMA proponents assume that reconnaissance drones, precision weapons, and glittering command and control centers can lift "the fog of war" to enable accurate targeting, which will shorten the duration of war and reduce casualties. A more recent and more pessimistic variant holds that advanced networked societies are vulnerable to devastating cyber-attack. Both views assume that IT radically empowers offensive control. Yet actual military organizations also experience frustration with incompatible software, micromanagement from continents away, failures to coordinate operations, accidental attacks on civilians, tragic fratricides and mistaken identities of targets on *PowerPoint* slides. IT "in the wild" doesn't operate as rationally as either RMA enthusiasts or cybersecurity alarmists believe.

RMA ideas grew out of the Cold War, but they really took off in the internet-fueled millennialism of the 1990s. The RMA became official U.S. doctrine under various guises as "network centric warfare," "information operations," and "defense transformation." In earlier eras, Guilio Douhet expected airplanes to directly attack a population's will to fight and thereby render land war irrelevant, and J.F.C. Fuller expected fleets of tanks to sweep infantry from the battlefield; both men ignored the strategic and social contexts of employment which shaped these new weapons and integrated them into existing ways of war.[2] The information revolution, likewise, neither compels military transformation nor favors particular operational concepts. Just as the dotcom crash of 2000 deflated some enthusiasm for the information revolution, so too have the protracted conflicts in Iraq and Afghanistan provided evidence against the original RMA vision of better fighting through technology.

Nevertheless, through these wars the U.S. military has continued to invest heavily in "C4ISR," the catchall term in U.S. doctrine for the IT-intensive functions of military operations:

---

[1] Carl von Clausewitz, *On War*, trans. and ed. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 102

[2] I. F. Clarke, *Voices Prophesying War, 1763-1984* (New York, NY: Oxford University Press, 1966)

command, control, communications, computers, intelligence, surveillance and reconnaissance. Apparently, practical-minded personnel still find IT useful in combat. The RMA debate doesn't explain when and how IT matters for military power, or why IT supports such highly variable performance on the battlefield. Neither side, pro or con, has looked closely into what a growing proportion of the military population actually does with all of that IT. The historical evolution of military IT has not been a revolutionary saltation but rather a gradual intensification of knowledge work: more people, more of the time, now experience war through a computer screen. The administration of violence increasingly resembles mundane office work rather than dramatic combat on the battlefield.

This dissertation explains why the technology that is supposed to reduce uncertainty often becomes a source of breakdowns, misperception, and politicization. I introduce the notion of *information friction* as an aggregate measure of factors—gleaned from the sociology of technology, security studies, and cognitive science literatures—that cause real information systems to diverge from technocratic ideals as personnel struggle to coordinate IT with the operational environment. I advance a range of hypotheses on the causes of information friction—the structure of the battlefield, the bureaucratic politics of technical protocols, and human-computer interaction—and its consequences for battlefield performance. The challenges of IT employment transcend the military domain, so this project should be of interest to students of technology and culture more generally. Information friction is a general phenomenon of the information age, but it is especially pernicious in war.

In order to observe the RMA in its natural habitat, I mobilized to active duty as a U.S. naval reserve officer and joined a special operations task force in Iraq's Anbar Province from 2007 to 2008. This participant-observation study examines the unintended consequences of pervasive IT, such as endemic coordination problems and the amplification of insular doctrinal preferences. To test the external validity of insights gained thereby, I also completed an historical study of the 1940 Battle of Britain. My fieldwork in Iraq demonstrates that high information friction and degraded performance is possible with sophisticated IT, while the Battle of Britain reveals impressive performance with far less sophisticated networks. The social context, not just the quality of the technology, makes all the difference. In addition, I include many shorter examples from recent military history to illustrate theoretical concepts.

This introduction will proceed in five parts: (1) a recent historical example to show why information friction matters; (2) an overview of information friction theory; (3) a summary of this dissertation's empirical methodology and findings; (4) a survey of the interdisciplinary contributions of this research; and (5) a short synopsis of the chapters ahead.

1.2 Consequences of Technological Misperception

Information processing blunders can have tragic consequences for international relations. On 7 May 1999, U.S. B-2 stealth bombers delivered satellite-guided weapons precisely to the coordinates that their higher-headquarters had approved. American intelligence officers believed this building to be the headquarters of the Serbian weapons procurement bureau, but only after it was in flames did they learn that it was actually China's embassy in Belgrade. The strike killed three *Xinhua* reporters and injured twenty others. In the aftermath, thousands of protesters in China hurled rocks at American diplomatic facilities, and Sino-American relations soured for months as Chinese officials accused the U.S. of a deliberate attack. Their suspicion was reasonable enough, as the bombs just happened to hit the defense attaché's office and the embassy's intelligence cell. The U.S. apologized for the mistake, blaming old maps and bad databases. To this day, however, most popular and elite opinion in China holds that so precise a strike by so advanced a military could not possibly have been an accident, so it must have been a veiled threat to intimidate Asia's rising power. The American blunder reinforced China's commitment to aggressive military modernization and exacerbated the spiral of mistrust between the two great powers.

As it turns out, the actual Serbian weapons bureau was just 300 meters south of the embassy. Congressional and journalist investigations revealed bad judgment and incompetence aplenty, but no deliberate targeting of China. How could so grievous an error occur? [3]

[3] The details of this account are drawn from Steven Lee Myers, "Chinese Embassy Bombing: A Wide Net of Blame," *New York Times* (17 April 2000); George Tenet, "DCI Statement on the Belgrade Chinese Embassy Bombing," House Permanent Select Committee on Intelligence Open Hearing, 22 July 1999; Eric Schmitt, "In a Fatal Error, C.I.A. Picked a Bombing Target Only Once: The Chinese Embassy," *New York Times* (23 July 1999).

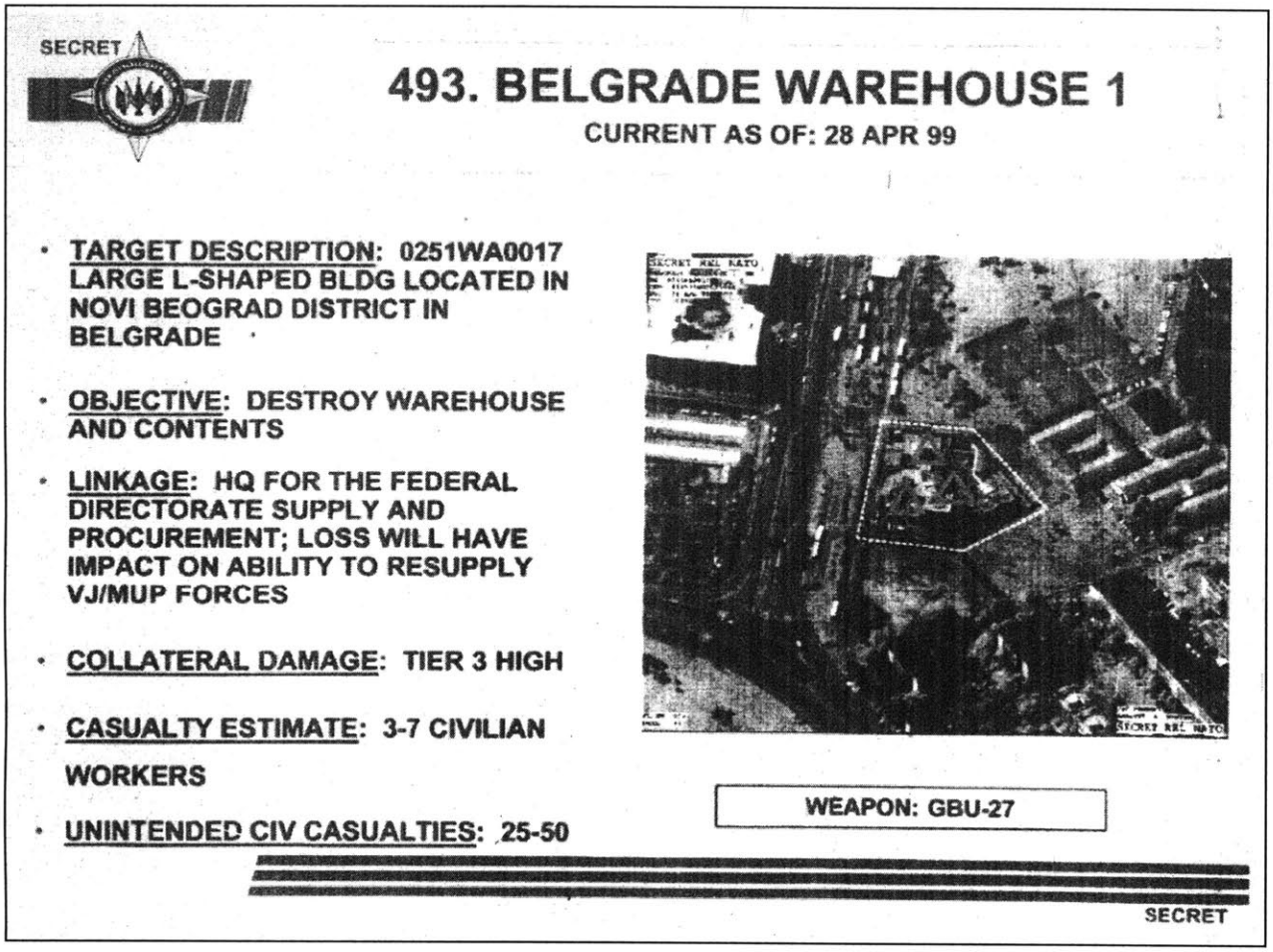


Figure 1-1: PowerPoint slide describing a NATO bombing target in Belgrade (*New York Times*)

The *New York Times* described the target as "an immense error, perfectly packaged."[4] Figure 1-1 is a *PowerPoint* slide of the target that turned out to be the Chinese Embassy. The slide describes target 493 from the "Master Target File" spreadsheet and has several features typical of the administration of violence: the "SECRET" security classification, a "basic encyclopedia number" (0251WA0017) in an intelligence database, a satellite image with *PowerPoint* triangles overlaid to indicate aimpoints, a vague "will have impact" statement about expected effects, a surprisingly accurate casualty estimate derived from computer models, and the corporate logo of U.S. European Command to signal authority and credibility.

The Belgrade supply directorate wasn't a particularly important target, but anything vaguely connected to the Serbian military was up for consideration in the hasty rush to identify "2,000 targets," the guidance from NATO commander Wesley Clark. Officers at the CIA saw an

[4] This slide is reprinted in Myers, "Chinese Embassy Bombing," A10

opportunity to deal with a tangential concern about Serb smuggling of missile parts to Libya and Iraq. They had a street address for the building reported by a human agent. In order to derive geographic coordinates, they used paper maps and made the assumption that addressing schemes on parallel streets followed a uniform standard (in hindsight incorrect). They checked the derived coordinates in several intelligence databases, but they found neither the Chinese embassy, for which they weren't looking, nor any other collateral damage concerns. It turns out that the Chinese had moved into the new embassy in 1996, and while diplomatic officials were surely aware of this, the news never percolated into intelligence channels to reflect the new reality that the Chinese had moved their embassy into the building with the anodyne name "Belgrade Warehouse 1" in the database. Imagery analysts furthermore failed to note any Chinese markings on the facility, but they weren't looking for them either.

The target was reported through several different channels, a situation intelligence officers call "circular reporting," where one report appears to be corroborated by others that are actually just repackaged copies of the first. The coordinates—delivered in a digital format with several digits of precision—appeared to be far more accurate than an intersection/resection estimate from a paper map could actually achieve. Furthermore, the target came with the authority of the CIA, even though the agency actually had little experience picking bombing targets. President Clinton approved a smartly-formatted *PowerPoint* slide which appeared to be as well vetted and verified as any of those for hundreds of other targets.[5]

Rational targeting processes were distorted from the start by impetuous targeting guidance and CIA opportunism. Each step in the chain of representations—reformatted and recombined across paper maps, databases, digital slides, and human minds—carried over earlier errors but removed evidence of them. As a result, American officers had an insular view of reality that bore little resemblance to facts on the ground. To be sure, individuals made mistakes and bad judgment calls aplenty, but the very complexity of the information architecture, sprawling across continental and bureaucratic boundaries, also contributed to the failure. The technological infrastructure of perception heightened the potential for misperception, and highly-leveraged precision weapons magnified its consequences.

---

[5] Prior to the strike, a CIA officer with misgivings about the target phoned military officers in Naples. The officers were led to believe that the target was merely a minor facility of the Serb weapons bureau, with no serious collateral damage alarm, so they opted to let the strike progress.

1.3 Overview of Information Friction Theory

The nineteenth-century Prussian army officer Carl von Clausewitz writes that "Friction is the only concept that more or less corresponds to the factors that distinguish real war from war on paper."[6] Likewise, information friction theory explains why real IT usage in war diverges from RMA ideals. Advanced militaries increasingly fight war on paper and *PowerPoint*, but the friction doesn't go away; on the contrary, new technology introduces new sources of friction. Before I define *information friction* more formally, I will first lean on Clausewitz to convey the intuition behind it.

1.3.1 Clausewitz in the Information Age

Clausewitz writes a great deal about the nature of practical knowledge and its limits.[7] Commanders often receive no information about crucial developments; or the information they receive is false; or it's true but arrives too late to be of any use; or they can't understand the meaning of the true information they do receive in time. Clausewitz describes this pervasive uncertainty as "the fog of war."[8] His notion of "general friction" includes "fog of war" along with the corrosive effects of physical danger and exhaustion, material breakdowns and bad luck, and political chafing within one's own organization.[9]

Even the most ardent RMA proponents expect some friction in war, but they believe that IT can relieve at least one component. The revealing title of Admiral Owens' book on the RMA

---

[6] Clausewitz, *On War*, 119

[7] Clausewitz anticipates many elements of 20th century philosophy of knowledge; John Tetsuro Sumida, *Decoding Clausewitz: A New Approach to On War* (Lawrence, KS: Kansas University Press, 2008), 94-112. Clausewitz was not trained in philosophy, although like many in his intellectual milieu, he was probably influenced indirectly by Kant and Hegel; Peter Paret, *Clausewitz and the State* (Princeton University Press, 1985), 147-208. Indeed, there is a Kantian feel to Clausewitz's quest to describe the "essence of the phenomena" of war and in his appeal to moral faculties or "genius." However, Clausewitz's epistemology has more in common with twentieth-century pragmatism and phenomenology than Cartesian rationalism or Kantian idealism, to say nothing of the contrast between Clausewitzian realism and Kant's idealistic "perpetual peace." On Clausewitz and contemporary critical theory see René Girard and Benoît Chantre, *Battling to the End [Achever Clausewitz]*, trans. Mary Baker (East Lansing, MI: Michigan State University, 2010).

[8] Clausewitz, *On War*, 140: "The general unreliability of all information presents a special problem in war: all action takes place, so to speak, in a kind of twilight, which, like a fog or moonlight, often tends to make things seem grotesque and larger than they really are. Whatever is hidden from full view in this feeble light has to be guessed at by talent, or simply left to chance. So once again for lack of objective knowledge one has to trust to talent or to luck."

[9] While "friction" is a mechanical term, Clausewitz first used the word to describe headquarters politics, not just broken wagons and bad intelligence. Peter Paret, "The Genesis of *On War*" in *Ibid.*, 16, explains that Clausewitz first used the term *friction* "during the campaign of 1806 to describe the difficulties Scharnhorst encountered in persuading the high command to reach decisions, and the further difficulties of having the decision implemented."

is *Lifting the Fog of War.*[10] Unfortunately, the very means used to reduce uncertainty themselves become additional sources of uncertainty, breakdown, and politicization. In wartime "things no longer run like a well-oiled machine," and "the machine itself begins to resist."[11] Information age discourse often describes information as a sort of "weightless" or "virtual" thought-stuff,[12] but in reality it is everywhere embodied in hardware, software protocols, piles of paper, and human brains. Glitches, bugs, incompatible formats, lost files, and emotional quarrels, to say nothing of enemy fires, wreak havoc on information processing. More complex IT has more ways to break down.

The twentieth century witnessed a pronounced shift toward knowledge work in military organizations, described in Chapter 2, which removes many personnel from direct encounters with violence. Robots and long-range weapons bear the brunt of reconnaissance and killing while humans build *PowerPoint* slides and work the remote controls. Many personnel are still exposed to roadside bombs and snipers on modern battlefields, to be sure, but technology has nonetheless limited exposure for more personnel more of the time. One unappreciated consequence of the technological abatement of danger, however, is the masking of clear signals of the presence of uncertainty. In a situation where men are dying close at hand and gear is strewn across the landing beach, then commanders can clearly perceive "something is wrong!" By contrast, uncertainty is not so visceral when commanders experience it, if at all, through several layers of staff and machine interpretation. The removal of danger tends to also remove clues that information is not reliable. While danger might be abated, physical exhaustion is not. Officers instead toil sleeplessly (which can only degrade the quality of decision-making) to fix *PowerPoint* briefs and negotiate dysfunctional human-computer networks. Bombarded by timely information from all directions about every niggling problem within tremendously complex organizations, officers become neurotic wrecks who "run around with their hair on fire" (in military argot) to address the breakdowns of the moment rather than the broader mission. Stultified with IT, they focus on immediately fixable problems and unimportant but available targets.

---

[10] William A. Owens and Edward Offley, *Lifting the Fog of War* (New York, NY: Farrar, Straus and Giroux, 2000)

[11] Clausewitz, *On War*, 104

[12] For example, Nicholas Negroponte, *Being digital* (New York: Knopf, 1995); Diane Coyle, *The Weightless World: Strategies For Managing the Digital Economy* (Cambirdge, MA: MIT Press, 1999); Eric S. Raymond, "Homesteading the Noosphere," *First Monday* vol. 3, no. 10 (1998)

Militaries adopt IT in order to lift the fog of war, but it also smuggles it in through the back door. A revision of Owens' book might be more accurately entitled "*Shifting* the Fog of War" because IT-intensive militaries spend tremendous effort debugging sprawling human-computer information systems, so the fog of war hangs within the mind of the organization itself. The obstinately mechanical and organic embodiment of information systems distinguishes real war from RMA fantasies of virtual victory.

Clausewitz believes that the only way to overcome debilitating friction is through moral and intellectual "genius." Personal experience in combat and the close study of military history develop a commander's intuition, perceptive *coup d'oeil*, and determination to perceive and seize opportunities amidst political and material chaos. If information friction is the persistence of Clausewitzian friction in IT-intensive war, then the expedient adaptation of information systems in the midst of using them is the information age manifestation of Clausewitzian genius. Because "it is simply not possible to construct a model" of the dynamic battlefield in advance, and because IT inevitably breaks down "no matter how versatile the code," personnel must "operate outside the rules" to meet unforeseen representational challenges.[13]

The daily fact of intensive improvisation and negotiation in knowledge-intensive militaries has remained largely invisible in popular and scholarly treatments of the RMA.[14] As U.S. Army officers observed during the 2003 invasion of Iraq, "the digital interface between the land and air components required tremendous human intervention to work....Despite the

---

[13] Clausewitz, *On War*, 140. The translation of "code", "model", and "rules" with their computational connotation is fortuitous, although the anachronism is duly noted. Clausewitz's full passage reads: "We must remind ourselves that it is simply not possible to construct a model for the art of war that can serve as a scaffolding on which the commander can rely for support at any time. Whenever he has to fall back on his innate talent, he will find himself outside the model and in conflict with it; no matter how versatile the code, the situation will always lead to the consequences we have already alluded to: *talent and genius operate outside the rules, and theory conflicts with this practice.*" Howard and Paret seem to translate *dasselbe* as "code" but it literally is just a reference to a previous noun, in this case *Lehrgebaeude*, which Howard and Paret translate as "model" but which might better be rendered as "teaching construct" to avoid the conceptual baggage of "model." I'm indebted to Paul Harris Wilt for this interpretation.

[14] Whereas the Clausewitzian genius is a romantic hero standing fast against chaos and uncertainty, expedient adaptation is a more distributed affair. Given the large staffs and standing intelligence bureaucracies so prominent in contemporary warfare, there are now many personnel caught up in knowledge work who must work through information friction and seize opportunities to improvise. John Robert Ferris and Michael I. Handel, "Clausewitz, Intelligence, Uncertainty and the Art of Command in Military Operations," *Intelligence and National Security* vol. 10, no. 1 (1995): 1-58, describe the emergence of a collaborative and intelligence-dependent style of command, rather than the iron determination of the Clausewitzian hero compensating for pervasive uncertainty.

multitude of systems, most headquarters defaulted to [Microsoft] *Office* software to create decision products or to communicate ideas most effectively."[15] To the extent that RMA success can be observed in proscribed situations on American battlefields, such as in "time-critical targeting" or "blue force tracking," a ferment of expedient adaptation behind the scenes makes it possible. User innovation is the only emollient for information friction in wartime.[16]

1.3.2 Consequences of Information Friction

In order for any organization—whether a tank crew or theater headquarters—to exert control on the battlefield, it must be able to *perceive* information about the world, *integrate* it with information stored in memory, *articulate* decisions to act in the world, and iterate this feedback cycle repeatedly (Figure 1-2). Through this *control cycle*, representations propagate through human minds and technological media in order to coordinate informational structure with the external structure of the battlefield. Edwin Hutchins describes this complex human-computer symbiosis as *distributed cognition*.[17]

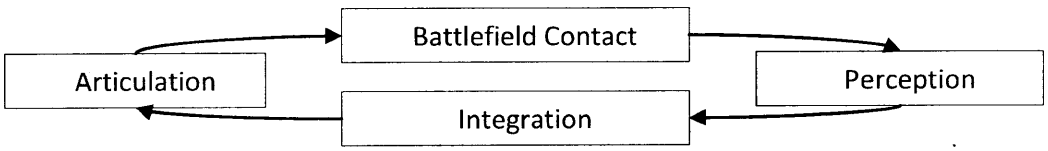


Figure 1-2: Information friction is breakdown in an organization's distributed control cycle

I define *information friction* as an aggregate measure of the risks for technical and political breakdowns throughout the distributed control cycle, to include agreement on the system's computational goals. It is the intensity of an organization's struggle to coordinate the structure of its representations of the world with the structure of the world itself. Information friction theory thus explains the conditions under which a distributed cognitive system can be smart or stupid. When information friction is low, then stable networks enable personnel to share information and improve their "situational awareness," which in turn improves operational

---

[15] Thomas L. Kelly and John P. Andreasen, "Joint Fires: A BCD Perspective in Operation Iraqi Freedom," *Field Artillery* (November-December 2003): 20-25

[16] Expedient adaptation is not a panacea, however; amateurism also generates negative reliability, interoperability, and security externalities which increase friction, discussed in Chapter 4.

[17] Edwin Hutchins, *Cognition in the Wild* (Cambridge, MA: MIT Press, 1995). The terminology for the phases of the control cycle comes from David A. Mindell, *Between Human and Machine: Feedback, Control, and Computing Before Cybernetics* (Baltimore, MD: Johns Hopkins University Press, 2002), 22-23, which draws on Hutchins' concepts to describe naval gunfire control and other military feedback systems.

control of the battlefield as per the optimistic expectations of RMA doctrine: systematic precision targeting, self-synchronizing maneuver, low casualties, shorter duration of conflict, and decisive, legitimate outcomes. Reliable information systems are necessary for militaries to enjoy "command of the commons" to dominate and deter competitors.[18] When friction is high, however, then personnel struggle through the "fog of war." Control cycles don't work as intended, and organizations can't agree on what their intentions are, which leads to tussles over technical protocols. Militaries with dysfunctional and politicized information systems operate in the "contested zone" with outcomes contrary to RMA expectations. Protracted contests of bloody attrition lead to ambiguous outcomes, and/or unreliable targeting causes "friendly fire," collateral damage, and other unfortunate consequences.

1.3.3 Causes of Information Friction

I organize the causes of information friction into the three "images" of international relations theory: strategic structure, bureaucratic politics, and individual behavior.[19] I do not consider "technology" as a separate exogenous factor because doing so quickly leads to the sort of technological determinism RMA proponents embrace and I am trying to avoid. Instead, I disaggregate aspects of technology across all three images, thereby putting IT into its social context.

1.3.3.1 External Stability

The battlefield is the object of knowledge. Is its objective structure clean or messy, durable or changeable? Does the technical state of the art make it possible in principle to connect with entities on the battlefield and retrieve records of that connection? Is the enemy's behavior predictable and lackluster, or confounding and relentless?

1.3.3.2 Internal Consensus

The subject which knows the battlefield is actually a complex collection of organizational actors. Do actors share doctrinal preferences about ends and means? Does the number and composition of actors frustrate coordination? Do stakeholders agree about how to integrate technical standards and protocols, or do they vie for control? Is the investment and

---

[18] Barry R. Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security* vol. 28, no. 1 (2003): 5-46

[19] Kenneth N. Waltz, *Man, the State, and War* (New York, NY: Columbia University Press, 1954)

implementation of technical architecture captured by rent-seekers and overtaxed with transaction costs?

1.3.3.3 Expedient Adaptation

In the course of turbulent wartime operations, personnel inevitably have to modify their information systems. Is IT extensible or locked to adaptation? Are there boundaries to technical expertise in forward areas where personnel encounter emergent information problems? Are personnel mindful of the positive and negative externalities of their adaptations? Do military institutions encourage bottom-up user innovation and improve upon prototypes that work?

1.3.4 Scope Conditions for the RMA

These factors suggest three conditions necessary for realizing the sort of performance enhancements that RMA doctrine expects from IT networks (Figure 1-2). Firstly, external stability requires that features of the battlefield must be knowable in principle. Secondly, internal consensus requires that actors agree about how to mobilize bureaucratic and technical resources to know the world. When both conditions are met, actors can coordinate "subjective" representations with the "objective" environment in order to thereby close control loops on the enemy. During wartime, however, it is inevitable that one or both of these conditions will fail. The enemy compromises external stability and bureaucratic tussles undermine internal consensus. Personnel then have to struggle with an information system that is uncoordinated with the structure of the world. Thirdly, therefore, the condition of expedient adaptation requires that an organization must be able to lower barriers between technical expertise and operational needs in order to reconfigure its sociotechnical information systems on the fly.

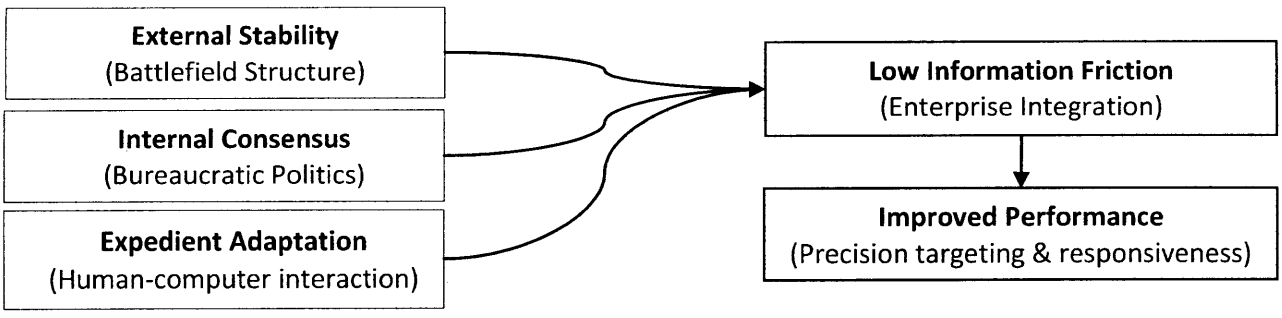


Figure 1-3: Conditions which promote low information friction and improved performance

Conversely, messy battlefields, controversies over technical protocols, and barriers to adaptation all raise information friction and thus degrade battlefield performance (Figure 1-4).

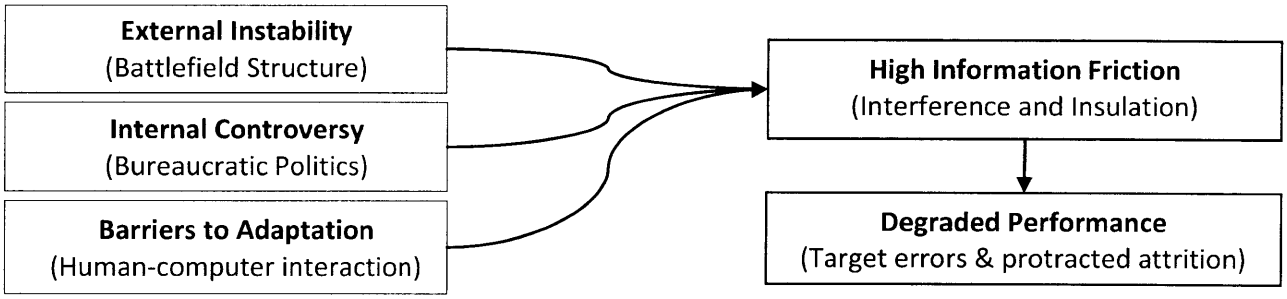


Figure 1-4: Conditions which promote high information friction and degraded performance

I will lay out all of the contextual factors beyond just the technical characteristics of IT that shape its usage and thus its contribution to battlefield performance. It is beyond my scope to explicitly treat the relative weight of all of these alternatives to technological determinism. I do briefly treat some interactions between them. Excessive internal consensus amidst external instability can lead to myopic insulation and the persistence of counterproductive behavior. Internal consensus and expedient adaptation are somewhat in tension because they exemplify, respectively, top-down regulation and decentralized interaction, which should be expected to have the strengths and weaknesses of hierarchies and markets in general. This tension is eternal, even as militaries become more complex in an effort to resolve it. Information systems are never complete, and expedient adaptation is always needed to adapt them to unforeseen circumstances. A major contribution of this project to the field of security studies is the organization a broad literature into accessible categories that highlight the ways in which structural, organizational, and individual level factors shape IT employment.

1.4 Empirical Methodology and Findings

This dissertation seeks to explain important battlefield outcomes, but to do so it takes a very granular focus on highly-situated interactions among people and machines. It's easy to take technology for granted because it is so pervasive, or by the same token to try and explain too much with technology alone. A major task here is simply to problematize the material embodiment of cognition and the social embedding of technology in everyday experience.

1.4.1 What Kind of Dissertation is this?

Stephen van Evera describes several types of political science dissertations and notes that most students combine theory building and theory testing, with significant emphasis on the

latter.[20] This dissertation, by contrast, combines substantial "stock-taking" and theory building with some detailed theory testing. I draw on a large literature outside of political science—especially the sociology of technology—and organize it into hypotheses on the causes and consequences of military IT usage patterns.[21] In addition to this theory building thrust, I also provide two detailed tests of the theory—U.S. special operations in Iraq and the 1940 Battle of Britain—to ensure that the mechanisms work as expected under very different conditions. Once we see that the theory has explanatory value in two radically different cases, we then gain confidence in it over technological determinism. I thus illustrate the plausibility of the theory, but I neither control for every permutation nor test every hypothesis exhaustively. I identify many structural, bureaucratic, and human-computer interaction factors which shape command and control systems beyond technical properties alone. Future research can explore their scope and interaction.

1.4.2 Ethnographic Fieldwork

The language of theory *testing* does adequately capture my use of participant-observation methods to *construct* information friction theory. My Iraq fieldwork provides a detailed test of the theory, but more importantly, personal immersion in information friction was crucial for my being able to articulate the theory at all. Ethnographic methods are invaluable for the study of uncontrolled real-life phenomena that are inadequately documented in archives or recalled in *post hoc* interviews. The concepts and processes which actually organize situated interactions often seem so natural, unremarkable, reflexive, or inaccessible to participants so as to be hidden in plain view. Similar to the way in which native speakers of a language can't explicitly articulate rules of their phonology and grammar, so do members of a group skillfully navigate their social world without being able to articulate the concepts that organize it.[22]

---

[20] Stephen W. Van Evera, *Guide to Methods For Students of Political Science* (Ithaca, NY: Cornell University Press, 1997)

[21] Prominent international relations works that leverage a large literature to generate theory, but without exhaustively testing it, include Kenneth N. Waltz, *Man, the State, and War* (New York, NY: Columbia University Press, 1954); Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976); Stephen W. Van Evera, *Causes of War: Power and the Roots of Conflict* (Ithaca NY: Cornell University Press, 1999)

[22] Michael H. Agar, *The Professional Stranger: An Informal Introduction to Ethnography, 2nd Edition* (Elsevier Academic Press, 1996). Ethnographers all deal with the fundamental problem of *reflexivity*, whereby the involvement of the observer influences and is influenced by the phenomena observed; see John Van Maanen, "The Fact of Fiction in Organizational Ethnography," *Administrative Science Quarterly* vol. 24, no. 4 (1979): 539-550;

There are many reasons why military knowledge management is poorly documented. The work that goes into debugging sociotechnical systems is self-hiding because the scaffolding is swept away as servers get reformatted and email accounts deleted in the normal course of operations. Many struggles and interactions with email, chat, and video teleconference are not recorded in archives at all. Data that does get archived—most of it trapped behind classification barriers—is difficult to comb through without an understanding of the use-context of all the different formats and genres.

Participant-observation provides a different way of bringing a theoretical instrument—the trained researcher—into a natural laboratory in order to measure the phenomenon of information friction. As Diana Forsythe observes, "the fieldworker herself is the research instrument, one which is 'calibrated' first through training in theory and methodology and then through experience. Learning to *do* ethnography involves learning to *see* social situations in a way that problematizes certain phenomena."[23] Ethnography provides immersive access to complex causal processes as they unfold. Prior theoretical preparation of the observer makes them visible, like a stain on microscope slide. Sometimes the hardest part of a research project is identifying and defining the phenomena and the variables of interest, especially when dealing with something as ubiquitously embedded in organizational life as IT.[24]

The country went to war in Iraq while I was in graduate school, and I happened to be an officer in the U.S. Naval Reserve. I thus saw an opportunity to immerse myself in an environment well-endowed with RMA resources so that I could see how IT was actually used in a combat zone. I volunteered for active duty and became a full-time member of a special operations task force in Iraq. While I was open about by civilian graduate student identity, I was a participant first and observer second. Fortunately, there was a natural synergy between my participant and observer roles. Military officers often have to switch their attention between

---

Isabella Baszanger and Nicolas Dodier, "Ethnography: Relating the Part to the Whole," in *Qualitative Research: Theory, Method and Practice*, ed. David Silverman (London: Sage Publications, 2004): 9-34; J.M. Roberts and T. Sanders, "Before, During and After: Realism, Reflexivity and Ethnography," *The Sociological Review* vol. 53, no. 2 (2005): 294-313; Pierre Bourdieu, *In Other Words: Essays Toward a Reflexive Sociology* (Stanford, CA: Stanford University Press, 1990) ; N. S. Mauthner and A. Doucet, "Reflexive Accounts and Accounts of Reflexivity in Qualitative Data Analysis," *Sociology* vol. 37, no. 3 (2003): 413-432.

[23] Diana E. Forsythe, *Studying Those Who Study Us: An Anthropologist in the World of Artificial Intelligence* (Stanford, CA: Stanford University Press, 2001), 148

[24] Susan Leigh Star, "The Ethnography of Infrastructure," *American Behavioral Scientist* vol. 43, no. 3 (1999): 377-391

what information means and *how information works* in order to stabilize IT and staff processes to make it possible to perceive the battlefield and control tactical forces. It turns out that knowledge workers often have to pay attention to the same types of things that an ethnographer of knowledge work cares about.[25] Chapter 5 further discusses the challenges of employment with the study group as well as limitations on fieldnotes and disclosure limitations due to classified information. There are surely formidable obstacles in this research strategy, but it also offers some unique opportunities to study the RMA in its natural habitat.

1.4.3 Empirical Findings

The Iraq case involves advanced IT networks in a Joint organization as well as extreme values on two of primary causes of information friction variables (external stability and internal consensus). This is a good test because a technological determinist RMA perspective would expect improved battlefield performance while my theory expects to see high information friction and degraded performance. The latter prevailed, highlighting the ways in which structural and organizational context shapes IT usage and its performance outcomes.

I found endemic collective action problems in the daily use of different forms of IT such as *PowerPoint,* email, shared file servers, internet browsing, *etc.* Public goods like well-organized information stores and reliable representations of the world were underprovided. When bureaucratic leadership tried to intervene to set standards, its solutions were often ill-suited to local situations, so users defected from the common scheme. As a result, information practices were often locally efficient but collectively irrational. Flexible IT on everyone's desktop, access to vast information networks, and difficult organizational coordination problems tended to make everyday information friction more intense. There was little technical expertise nurtured for or dedicated to the problem, and so information management was incredibly *ad hoc.*

More seriously for military effectiveness, information processes tended to reinforce doctrinal preferences for high-risk, high-prestige commando behavior. Organizational behavior became insulated from and sometimes inimical to broader U.S. counterinsurgency goals in Anbar province. The pursuit of ever more raid targets submerged the intelligence or methodological errors in complex information processes and instead reified a simpler, more coherent view of the

[25] Ulrike Schultze, "A Confessional Account of an Ethnography about Knowledge Work," *MIS Quarterly* vol. 24, no. 1 (2000): 3-41

world in *PowerPoint* slides. Information friction frustrated the creation of reliable information products, but as the organization was strongly inclined to develop products that justified "direct action" missions, it did so without attending to flaws in their construction. The relative autonomy, resources, and secrecy of special operations enabled the organization to indulge its preferences. Operational effects against the insurgency and within local populations were difficult to assess as the organization instead measured its own performance.

1.4.4 External Validity

A single detailed and theoretically-grounded case is valuable for the theory-*constructing* phase of social scientific inquiry, but it raises questions of external validity for theory-*testing*.[26] Validity concerns can be mitigated somewhat by the fact that ethnographic research is not just isolated observation, but theoretically-grounded attention to the ways in which empirical data suggests modification of existing theory.[27] Fieldwork, as with archival research, provides a sort of "folk Bayesian" update of an existing body of scholarship by asking whether current conditions differ from past interpretations.[28] Nonetheless, one might reasonably wonder how well information friction theory travels outside of the dusty terrarium of Anbar province and its unique special operations subculture. I intend the theory to explain the performance of military information systems across a broad spectrum of conflict. Thus it is important to perform an external validity test.

To choose a case to contrast with the Iraq study I looked for more rudimentary IT but more impressive battlefield performance. Given less sophisticated IT, a simple technological determinist perspective would expect lower performance levels. A case with impressive performance would obviously invalidate that expectation, but furthermore, I would need to check whether the context of IT usage mattered the way information friction theory says it should. I chose the 1940 Battle of Britain because of its electromechanical and paper IT and because historians largely agree that Fighter Command's integrated air defense system deserves much credit for winning the battle. British adoption of radar and communication networks provided

---

[26] John Gerring, *Case Study Research: Principles and Practice* (New York, NY: Cambridge University Press, 2007), 39-43

[27] *Ibid.*, 146-162; Barney G. Glaser and Anselm Strauss, *Discovery of Grounded Theory: Strategies For Qualitative Research* (Chicago, IL: Aldine Publishing Co., 1967)

[28] Timothy J. McKeown, "Case Studies and the Statistical Worldview: Review of King, Keohane, and Verba's Designing Social Inquiry: Scientific Inference in Qualitative Research," *International Organization* vol. 53, no. 1 (1999): 161-190

improved their situational awareness and rapid decision-making. British fighters outfought the Germans because they knew more. When we look at the details of this case, therefore, we should see all three conditions of information friction theory met, or else we have to reject the theory. This case is an intrinsically important and well documented episode, and an extensive body of historical literature provides the granular level of detail needed to measure information friction. My theory must be able to pass this important "hoop test."[29]

The SOTF in Iraq was a robustly-networked beneficiary of the RMA, and yet IT usage created internal confusion and reinforced patterns of activity that were, at best, difficult to evaluate for effectiveness, and at worst, counterproductive for the overall U.S. counterinsurgency effort. Fighter Command, by contrast, operated in a pre-digital era with temperamental radar sets, voice radio, and manually-updated maps; nevertheless, this network produced a then-unprecedented level of shared situational awareness and rapid decision-making which proved critical in defeating the Nazi air offensive. Thus an "information age" organization generated less than stellar results, while an "industrial age" organization achieved RMA-like performance. The difference lies in the relative stability of the problem, agreement about the solution, and capacity to debug operational information systems in wartime.

I cannot test all of the combinations of variables described by the theory in this dissertation, but now we know the theory can plausibly explain two very different cases in detail. To further illustrate the plausibility of theoretical concepts as I introduce them, I also use many short examples from recent military history in Chapters 2 through 4. Information friction theory can provide explanatory value across radically different sociotechnical contexts, thus giving us confidence in its generalizability.

1.5 Interdisciplinary Contributions

This project bridges multiple academic disciplines and contributes to several different debates. The simple question, "Does technology improve knowledge in military organizations?" begs more complicated questions about the nature of technology in society, the relationship between individual and collective knowledge, the evolution of bureaucracies which manage violence, and the meaning of the information revolution for political institutions in general. In addition to these more profound questions, this project is also motivated by policy debates over

[29] Van Evera, *Guide to Methods*, 30-32, 86-87.

the "revolution in military affairs" (RMA) and "defense transformation," increasing investment in "cybersecurity," and the conduct of irregular warfare by high-tech militaries. I don't pretend that this project can adequately address all of these topics in depth, but I will take a few pages to show how, by virtue of my theoretical and empirical material, this dissertation inevitably touches upon them all.

1.5.1 Information Technology and Security Studies

A number of concerns in the security studies field surround IT and military power. Chapter 2 describes how the RMA debate has stalled out without much improving our understanding about how and when IT matters for battlefield performance, and "network centric warfare" has simply become the new normalcy. Yet my project also has broader implications for security studies beyond just the RMA debate.

1.5.1.1 Military Power and Effectiveness

RMA doctrine holds not only that the information revolution has enhanced U.S. military power, but also that further transformation is necessary to prevent other actors—rising powers like China, regional spoilers like Iran, or non-state villains like al-Qaeda—from leapfrogging ahead. This dissertation agrees that reliable information systems do indeed enhance "command of the commons," as Barry Posen describes U.S. military dominance in the sea, air, and space domains, but only under some conditions; naïve faith in IT can also exacerbate the frustration experienced in "contested zones" when those conditions are not met.[30] Information friction theory thus contributes to scholarship on the sources of military power and battlefield effectiveness.[31] The implication for U.S. foreign policy of an appreciation of information friction is that a grand strategy of restraint should seem more attractive than global primacy, the costs of which have been underestimated.[32]

---

[30] Posen, "Command of the Commons"

[31] Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton University Press, 2004); Risa Brooks and Elizabeth A. Stanley, *Creating Military Power: The Sources of Military Effectiveness* (Stanford, CA: Stanford University Press, 2007); Allan R. Millett, Williamson Murray and Kenneth H. Watman, "The Effectiveness of Military Organizations," *International Security* vol. 11, no. 1 (1986): 37-71; Martin Van Creveld, *Fighting Power: German and U.S. Army Performance, 1939-1945* (Greenwood Press, 1982)

[32] Barry R. Posen and Andrew L. Ross, "Competing Visions for U.S. Grand Strategy," *International Security* vol. 21, no. 3 (1997): 5-53, refers to restraint as "selective engagement."

1.5.1.2 Offense-Dominance

The RMA vision describes global reconnaissance and strike capabilities that enable rapid, low-cost "shock and awe" victories. Steven van Evera and other defensive realists argue that war is more likely when offense is easy or perceived to be easy.[33] The most dangerous situation is when technologies favor the defense but military doctrine favors offense. World War I is the most-cited example, as the "ideology of the offensive" among major combatants in Europe foundered upon impenetrable machine gun fire and artillery bombardment in the trenches.[34] This dissertation implies that the RMA is not an unmitigated boon for the offense because information friction degrades the reliability of organizational perception and sometimes traps militaries in counterproductive patterns of behavior. Belief in RMA offense-dominance increases the likelihood of prolonged wars with unfortunate and unintended consequences. Modern IT networks are indeed a permissive condition for command of the commons, but they should be employed with some humility and respect for their limitations.

1.5.1.3 The Inflated Cyberwarfare Threat

A persistent variation on the RMA theme is that IT networks have become both the means and target of a new kind of warfare. The dependence of advanced industrial countries on IT and the interconnection of globalized economies supposedly make them vulnerable to devastating attacks from state or non-state hackers who could paralyze society.[35] The U.S. has recently stood up U.S. Cyber Command—led by the director of the National Security Agency—to coordinate computer network attack and defense right alongside the NSA's experts in network exploitation for intelligence. Does the cyber threat justify the danger to civil liberties?

This dissertation does not take on cyberwarfare problems directly, but it does have important implications. Fear about crippling cyberattack is just RMA enthusiasm in reverse. Real information systems, by contrast, are often irrational messes with important interactions hidden in local social practice. Complex organizations already deal with dysfunctional IT and power failures (and lay waste to global financial systems without any nefarious help), yet they

---

[33] Stephen W. Van Evera, *Causes of War: Power and the Roots of Conflict* (Ithaca NY: Cornell University Press, 1999)

[34] *Ibid.*; Jack L. Snyder, *The Ideology of the Offensive: Military Decision Making and the Disasters of 1914* (Ithaca, NY: Cornell University Press, 1989). The offense-defense bias of technology has been challenged by Keir A. Lieber, *War and the Engineers: The Primacy of Politics Over Technology* (Ithaca, NY: Cornell University Press, 2005)

[35] Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York, NY: Harpercollins, 2010); Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001)

keep on muddling through, and militaries keep on fighting. Cybersecurity is assumed to be offense-dominant for tactical hackers, but is probably far less so at the systemic level. Cyber fear mongers assume that offense is easier than it actually is, and they underestimate the resilience of sociotechnical systems. Detailed discussion of these complicated matters is beyond my scope, but an appreciation of information friction might help to temper the hyperbolic cybersecurity debate.

1.5.1.4 Military Innovation and Bottom-up Change

The RMA debate has encouraged inquiry into the sources of military innovation.[36] The primary explanations include intervention by civilian leaders in response to changes in the balance of power,[37] peacetime reform of military institutions,[38] and interservice rivalry over prestige and budget share.[39] Other scholars have emphasized culture, industrial structure, civil-military relations, and the diffusion of ideas and material.[40] All provide alternatives to technological determinism, but they do so in part by defining innovation as discontinuous *doctrinal* change.[41] They all tend to examine cases of large-scale technologies like ships, tanks, and missiles. Largely missing is consideration of the sort of bottom-up change that is so

---

[36] I am referring primarily to work by political scientists offering generalized theories of military innovation. There is also a rich historical literature on particular cases of military innovation; see, *inter alia*, Merritt Roe Smith, *Military Enterprise and Technological Change: Perspectives on the American Experience* (Cambridge, MA: MIT Press, 1985); William G. McNeill, *The Pursuit of Power: Technology, Armed Force, and Society Since A.D. 1000* (University of Chicago Press, 1982); Macgregor Knox and Williamson Murray, *The Dynamics of Military Revolution, 1300-2050* (Cambridge University Press, 2001).

[37] Barry R. Posen, *Sources of Military Doctrine: France, Britain and Germany Between the World Wars* (Ithaca, NY: Cornell University Press, 1984)

[38] Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca, NY: Cornell University Press, 1991)

[39] Owen R. Cote, "The Politics of Innovative Military Doctrine: The U.S. Navy and Fleet Ballistic Missiles," Ph.D. Dissertation, MIT Department of Political Science (1996); Harvey M. Sapolsky, "On the Theory of Military Innovation," *Breakthroughs* vol. 9, no. 1 (2000): 35-39; Harvey M. Sapolsky, *The Polaris System Development: Bureaucratic and Programmatic Success in Government* (Cambridge, MA: Harvard University Press, 1972)

[40] Elizabeth Kier, *Imagining War: French and British Military Doctrine Between the Wars* (Princeton, NJ: Princeton University Press, 1999); Matthew Evangelista, *Innovation and the Arms Race: How the United States and Soviet Union Develop New Military Technologies* (Ithaca, NY: Cornell University Press, 1988); Deborah D. Avant, *Political Institutions and Military Change: Lessons From Peripheral Wars* (Ithaca, NY: Cornell University Press, 1994); Emily O. Goldman and Leslie C. Eliason, ed., *The Diffusion of Military Technology and Ideas* (Palo Alto, CA: Stanford University Press, 2003); Peter J. Dombrowski and Eugene Gholz, *Buying Military Transformation: Technological Innovation and the Defense Industry* (New York, NY: Columbia University Press, 2006)

[41] The importance of doctrine in shaping military technology was established by Irving Brinton Holley, *Ideas and Weapons* (New Haven, CT: Yale University Press, 1953)

prevalent among smart military users of flexible commercial IT.[42] This dissertation does not seek to directly explain innovation *per se*, but it does argue that a ferment of low-level improvisation—what Eric Von Hippel calls "user innovation"[43]—is an important empirical fact of modern IT-intensive warfare. User innovation has been largely overlooked in both RMA and military innovation debates, but it is what makes any sort of real RMA performance possible.

1.5.2 Perception and Misperception

A principal difficulty in explaining how IT matters for military power is that computers are ubiquitous intermediaries in almost everything a modern military does. Wherever people need to communicate, plan, track, or persuade in organizations we find them manipulating IT. Intelligence data-mining, tactical control systems, network administration bureaucracy, and all the productivity software infused into military staffs have become so pervasive and complex that nobody can possibly understand how the whole system works. Some students of military affairs are thus tempted to attribute too much causal import to computers because they are everywhere (especially those worried about cybersecurity), while others ignore them in the same way that we take oxygen for granted. Similarly, many IT users are like fish oblivious to the ocean in which they swim. IT does not uniquely determine any particular outcomes by itself because it is so deeply embedded in social practice. Nevertheless, it does constrain and enable much of what an organization does, especially where perception is involved.

1.5.2.1 Technological Bias

An established line of research in security studies focuses on psychological biases in intelligence analysis and policymaking.[44] Organizational pathologies—to include deliberate deceit and manipulation—are another source of misperception.[45] However, the role of technology as a carrier of assumptions about the world has been largely overlooked. Electronic databases and graphical interfaces necessarily include design assumptions about what sort of

---

[42] Adam Grissom, "The Future of Military Innovation Studies," *Journal of Strategic Studies* vol. 29, no. 5 (2006): 905-934, notes this lacuna in his useful review of the debate. He also notes that the top-down vs. bottom-up distinction may obscure the fractal nature of innovation theories, with competition, intervention, and subcultures all playing a role at any scale. I agree but would add that IT tends to create such ferment at quite granular scales.

[43] Eric Von Hippel, *Democratizing Innovation* (Cambridge, MA: MIT Press, 2005)

[44] Robert Jervis, *Perception and Misperception in International Politics*; Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, DC: Center For the Study of Intelligence, 1999); Alexander P. Butterfield, "The Accuracy of Intelligence Assessment: Bias, Perception, and Judgment in Analysis and Decision," Naval War College Paper (March 1993)

[45] Stephen W. Van Evera, "Why States Believe Foolish Ideas: Non-Self-Evaluation By States And Societies," MIT Security Studies Program Working Paper, 10 January 2002

things on the battlefield should be tracked and how to track them. In deciding what is important, architects must also decide what to ignore, a decision that is often implicit and unintentional. Modern command and control systems put many layers of automated interpretation—as well as unrecorded human deviance from standards—between the collection of battlefield information and its apprehension by decision-makers. This lens enables sophisticated perception, but for the same reason also heightens the risk of misperception when representation and reality drift apart.

1.5.2.2 Intelligence Studies

The intelligence studies subfield of international relations has generally focused on the history of particular agencies and espionage intrigue rather than explanatory theory.[46] While there has been plenty of work on problems of cognitive bias as well as histories of particular technical collection disciplines, there has been little theoretical attention to the material culture of intelligence. This is odd because the practice of intelligence is thoroughly immersed in technologies for knowing and representing the world. This dissertation provides some insight into when intelligence work should be expected to clarify more than it obfuscates. I also shed some light on what it means to do military intelligence at a working level. One intelligence officer said to me that while the popular image of intelligence might be the exciting life of the character Jack Bauer on the television show *24*, a more accurate description of his life would be the "PC LOAD LETTER" scene from the movie *Office Space*.[47]

1.5.3 Political Control of Technical Protocols

There is a fundamentally political problem at the heart of any information system. IT networks enable collaboration...*if* people agree to adhere to the same technical protocols. Technical standards facilitate coordination across time and space, but they also provide competitive advantage (just ask Microsoft or Intel). Modern IT does not determine the outcome of standards fights, but with all of its complex layering and flexible connectivity, IT does catalyze the emergence of more actors and more types of actors to get into fights.

---

[46] David Kahn, "An Historical Theory of Intelligence," Intelligence and National Security vol. 16, no. 3 (2001): 79-92; Peter Gill, Stephen Marrin and Mark Pythian, *Intelligence Theory: Key Questions and Debates* (New York, NY: Routledge, 2009); Jennifer E. Simms, "A Theory of Intelligence and International Politics" In *National Intelligence Systems: Current Research and Future Prospects*, ed. Gregory F. Treverton, and Wilhelm Agrell (New York, NY: Cambridge University Press, 2009), 58-92

[47] *24* would furthermore have to be renamed "96" to include all the hours needed for Jack Bauer to do his paperwork and *PowerPoint* slides.

1.5.3.1 Systems Engineering

Technocratic advocates of "enterprise integration" often assume away the political problems, but system design and implementation is usually rife with bureaucratic tussle.[48] There are collective action problems in even the most mundane interactions with IT. Furthermore, engineers should be aware of the value-laden design decisions they make, as well as of the need to engineer not just technology but institutional support for it.[49] Politics goes all the way down in IT, so there is no clean distinction between the "technology layer" and the "policy layer" of information systems. Reforms of IT acquisition and management institutions should include operational users as partners in ongoing system design—through open source architectures, prototyping toolkits, and engineers forward deployed—in order to dampen some of the turbulence. This dissertation offers information system engineers a rough overview of the political minefield.

1.5.3.2 The Social Construction of Technology

My argument about the political nature of IT has an affinity with the "social construction of technology" school in the history and sociology of technology literature, from which I draw heavily in Chapter 3. Yet sometimes this perspective overcorrects against technological determinism to embrace a thoroughgoing relativism. Military organizations provide an interesting Petri dish for students of technology and organizations because they are so complex and technology-dependent. They also deal with such lethal consequences that it's hard not to bring in a little realism. This dissertation walks a fine line in using realist concepts (in the international relations sense of the distribution of power) as well as the political economy of technical standards to explain how military organizations use IT to construct their versions of reality. Beyond showing how a sociotechnical system is complex, we would also like to be able to explain the conditions under which the system might follow one trajectory or another. Moreover, a purely critical perspective doesn't provide a lot of traction for suggesting policy reforms to improve performance (or at least avoid blunders). Policies are essentially ideas about how to cause desirable outcomes, so sound policy should be built on hypotheses of cause and effect.

---

[48] David D. Clark, John Wroclawski, Karen R. Sollins and Robert Braden, "Tussle in Cyberspace: Defining Tomorrow's Internet," *IEEE/ACM Transactions on Networking* vol. 13, no. 3 (2005): 462-475

[49] John Law, "Technology and Heterogeneous Engineering: The Case of Portuguese Expansion," in *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*, ed. Wiebe Bijker, Thomas P. Hughes, and Trevor Pinch (Cambridge, MA: MIT Press, 1987), 111-134

1.5.3.3 Technology and Democracy

A major irony of RMA discourse is that it embraces information age rhetoric about the democratizing power of IT—the internet empowers people to collaborate and self-organize without rigid hierarchies—yet the RMA mobilizes this to enhance military power, the exemplar of state coercion! "Information wants to be free," so goes the techno-libertarian mantra, and indeed citizens sometimes do use new media to subvert government control.[50] Yet governments have long sought the latest IT to better improve their ability to monitor, compare, and tax their populations.[51] The dichotomy is false, as there are strengths and weaknesses in both the centralized and decentralized modes of IT employment, as in governments and free markets more generally. Modern IT certainly does empower small-scale actors to manipulate their information systems with alacrity, but at the same time the negative externalities they generate (problems in interoperability, reliability, scalability, and security) prompt hierarchical authorities to establish standards and controls. IT empowers both bottom-up and top-down modes of control, yet for that very reason it also exacerbates the tension between them, as well as the complexity of control struggles. This dissertation focuses on battlefield operations by military organizations, but it speaks to this larger societal debate over technology and democracy.

1.5.4 Irregular Warfare

By virtue of my fieldwork in Iraq, this dissertation should also be of interest to students of special operations forces (SOF) and counterinsurgency. As a practitioner I drew on the political science literature on civil war to try and understand what we were dealing with in Anbar province,[52] and this sensitized me to the broader political and information problems of counterinsurgency, which are ill-served by a myopic focus on killing bad guys.

---

[50] Some of the most breathless IT futurism is collected in Adam Brate, ed., *Technomanifestos* (New York: Texere, 2002), and treated more critically by Vincent Mosco, *The Digital Sublime: Myth, Power, and Cyberspace* (Cambridge, MA: MIT Press, 2004)

[51] James C. Scott, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed* (New Haven, CT: Yale University Press, 1998); Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (New York, NY: Oxford University Press, 2006); Shanthi Kalathil and Taylor C. Boas, *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule* (Washington DC: Carnegie Endowment for International Peace, 2003)

[52] Two texts I found particularly valuable in my practitioner role were Roger D. Petersen, *Resistance and Rebellion: Lessons From Eastern Europe* (New York, NY: Cambridge University Press, 2001) and Stathis N. Kalyvas, *The Logic of Violence in Civil War* (Cambridge University Press, 2006)

1.5.4.1 Special Operations: Caveat Emptor

U.S. Special Operations Command (SOCOM) has been growing at a rapid pace since the end of the Cold War and especially after 9/11. By 2015 "the fifth service" is projected to have 65,000 personnel, nearly a third the present size of the Marine Corps.[53] SOCOM's counterterrorist commandos and unconventional warfare experts (who interact with indigenous groups and conduct civil-military operations) are more and more seen as the weapon of choice against America's irregular and clandestine foes around the world. Such a balanced portfolio is indeed promising and surely more sustainable than large-scale deployment of conventional Army and Marine forces for counterinsurgency as in Iraq and Afghanistan.[54] Yet there is a problem, as Chapter 5 explains, in SOCOM's strong doctrinal preference for high-risk, high-prestige commando operations and its consequent underinvestment in important "non-kinetic" capabilities like tribal engagement and civil affairs. The secrecy, autonomy, and generous funding of special operations forces (SOF) allow them to indulge this preference, which often carries negative externalities for broader counterinsurgency goals and neglects alliance-building opportunities. Special operators are amazing tactical soldiers, but they should not be looked at as a panacea for the political problems of irregular warfare.

1.5.4.2 Technology and Counterinsurgency

The U.S. Army and Marine Corps have embraced "population-centric" approaches to counterinsurgency in Iraq and Afghanistan, as exemplified in U.S. Army *Field Manual 3-24*. The high-tech remote-control targeting emphasis of RMA doctrine appears quite ill-suited to "winning hearts and minds," and U.S. overreliance on American technical advantage has been derided by critics both within and outside the military.[55] However, the IT story on the ground is more complicated. IT is everywhere on the modern irregular battlefield, but not always along the lines of the RMA vision. Overhead reconnaissance platforms, ground sensors, and population census and biometric databases strive to provide "persistent surveillance" of a truly-

---

[53] "Michael Vickers Interview," *Defense News* (22 March 2010). The 2011 congressional budget authorizes 202,100 Marines.

[54] Austin Long, "Small is Beautiful: The Counterterrorism Option in Afghanistan," *Orbis* vol. 54, no. 2 (2010)

[55] Noah Shachtman, "How Technology Almost Lost the War: In Iraq, the Critical Networks Are Social—Not Electronic," *Wired* (27 November 2007); H.R. McMaster, "Crack in the Foundation: Defense Transformation and the Underlying Assumption of Dominant Knowledge in Future War," U.S. Army War College Center For Strategic Leadership Student Issue Paper S03-03, November 2003

Orwellian character.[56] Armed Predator drones patrol the tribal areas of Pakistan to hunt al-Qaeda operatives. "Blue force tracking" monitors daily patrols, and "information operations" exploit local communications infrastructure. Staff officers rely on Microsoft *Office* to plan and control "kinetic" raids and civil affairs missions alike. The adversary, moreover, has embraced commercial IT for internal administration, Google maps for mission planning, and the internet for coordination and propaganda. IT has been and can be mobilized in many different and surprising ways. Modern counterinsurgency is hardly low-tech, and the dichotomy between technology and indigenous engagement is a false one.

1.6 Roadmap

To sum up, this interdisciplinary project addresses broad questions about technology and war in the information age, but it approaches them carefully through detailed ethnographic and historical case studies. It offers a range of hypotheses on the performance of military information systems, but it does not test them all in depth. I have opened up many lines of fruitful inquiry for future research. The substantive chapters will proceed as follows.

Chapters 2 through 4 provide literature review, historical background, and the details of information friction theory. Chapter 2 summarizes the RMA debate, which has narrowly focused on the mixed performance of IT on the modern battlefield, rather than the growing percentage of the workforce in information processing jobs. Chapter 3 defines the notion of information friction, specifies its empirical manifestations in distributed cognition, and develops hypotheses on friction and battlefield performance. Chapter 4 describes the causes of information friction in the structure of the battlefield, bureaucratic politics, and human-computer interaction. The notion of information friction encompasses recursive interactions between IT infrastructure and human interpretation, but for analytical clarity, Chapter 3 first treats it as an independent variable, and then Chapter 4 treats it as a dependent one.

Chapters 5 through 8 are the empirical studies of the theory in action. Chapter 5 provides an introduction to U.S. SOF and the war in Anbar. After a discussion of methodological concerns, it measures the three causal variables and frames expectations for information friction.

---

[56] Martin C. Libicki, David C. Gompert, David R. Frelinger and Raymond Smith, *Byting Back: Regaining Information Superiority Against 21st-Century Insurgents, RAND Counterinsurgency Study, Volume 1* (Santa Monica, CA: RAND Corporation, 2007)

Chapter 6 describes the collective action problems that arose in the usage of various IT. Chapter 7 describes representational practices in special operations targeting, emphasizing how IT usage contributed to an insular target-focus amidst a more complicated counterinsurgency. Chapter 8 conducts an external validity test with the 1940 Battle of Britain, drawing mainly on secondary sources, to show how information friction emerges from fundamental organizational dilemmas rather than features of a particular technology.

Chapter 9 provides theoretical evaluation and policy recommendations. Modern IT doesn't determine performance improvements but only makes timeless dilemmas more acute by increasing their complexity. While the fundamental tensions of IT usage cannot be avoided, better attention to them as organizations become more dependent on IT can help to dampen the severity of oscillations between desirable and pathological outcomes.

Chapter 2: The Revolution in Military Affairs

> "The most unfortunate of all supreme commanders is the one who is under close supervision...a telegraph wire attached to his back." – Field Marshall Helmuth von Moltke ("the Elder")[1]

2.1 Increasing Knowledge Intensiveness

Great power militaries have been eager adopters of information technology (IT) for well over a century. Long before the internet and certainly after it, emerging IT has inspired visions of better knowledge and control of the battlefield. At the same time, uncertainty and confusion have remained central in experience of actual war. Over the last two decades in American defense circles, enthusiasm for a "revolution in military affairs" (RMA) has waxed and waned as popular excitement about the information economy in the 1990s gave way to protracted warfare in Afghanistan and Iraq in the 2000s. Yet hope springs eternal as personnel look to larger bandwidths, greater storage, and novel applications to address their wartime information needs.

Debates over whether IT is either good or bad for military effectiveness often overlook the profound long-term changes in military organizations which accompany the pervasive adoption of IT. Increasing IT usage is just part of a broader historical trend of increasing knowledge intensiveness. Throughout the last century militaries have developed larger headquarters staffs, greater dependence on planning and intelligence, increased automation of weapons, and more personnel in information processing roles rather than physical combat. This chapter will sketch out these historical trends and review the policy and academic debates over what they mean. There are reasons to be both optimistic and pessimistic about military IT, and thus the perennial RMA debate is ultimately irresolvable, even as IT-intensive operations have become the norm.

2.1.1 From Command to C4ISR

Throughout most of military history, "command" referred to the mental and moral qualities of a single commander. The man on horseback watched the battle unfold with his own eyes, and his mind was the principle information-processing organ of the army. In the eighteenth and nineteenth centuries, the information-processing burden of command increased as a clutch of industrial innovations such as reliable musketry, mobile artillery, improved roads, and railroads

[1] Daniel J. Hughes, ed., *Moltke on the Art of War: Selected Writings* (Novato, CA: Presidio Press, 1993), 77

expanded the scope and scale of warfare. At the same time other developments in cartographic science, telegraphy, and bureaucratic administration enhanced the supply of information-processing power. The functions of command thus overflowed the brain of the commander to involve a far more distributed collection of staff officers and information technology (IT), while the experience of command attended to the battlefield more indirectly through maps and reports. Dallas Irvine describes this profound shift:

> The art of war therefore became, in a sense that it had not been before, an art to be pursued upon the map, and with an immensely greater number of permutations and combinations possible than ever before. Obviously, the conduct of war upon this level required a far different order of intelligence, knowledge, preparation, and skill than the command of a visible mass of men upon a visible terrain. The first requisite under the new conditions was adequate maps. The second was a service of information to replace the former direct visual oversight by the commander-in-chief, a service which had to be provided, in part by reconnaissance officers and in part by written reports from subordinate commanders. A third necessity was a system of issuing written, instead of verbal, orders. The conduct of operations thus began to be a matter of written documents as well as of maps. The new situation consequently required a specially competent and more or less considerable staff to assist the commander in the exercise of his functions, and such a staff to be very effective would need to be trained in time of peace.[2]

Spencer Wilkinson—writing in 1891 to encourage Britain to expand its general staff after the German model—portrays the headquarters staff as "the brain of the army" which "can perform its functions only in connection with a body adapted to its control."[3] Infantry regiments and artillery battalions were organized so as to be legible and controllable through the communicative and representational means available to the headquarters staff. Naval command similarly shifted from the iconic captain with a spyglass on spray-washed decks into enclosed combat information centers for gunfire control and navigation.[4] As machine guns and howitzers improved the range and lethality of fire, as internal combustion and steam engines enhanced

---

[2] Dallas D. Irvine, "The Origin of Capital Staffs," *Journal of Modern History* vol. 10, no. 2 (1938), 173-174

[3] Spencer Wilkinson, *The Brain of an Army* (London: McMillan & Co., 1891), 97. Trevor Dupuy, *A Genius For War: The German Army and General Staff, 1807-1945* (Englewood Cliffs, NJ: Prentice-Hall, 1977), similarly uses the Clausewitzian term "genius" for the commander's moral faculties to describe an entire staff organization. See also James. D. Hittle, *The Military Staff: Its History and Development* (Harrisburg, PA: Stackpole Company, 1961)

[4] Timothy S. Wolters, "Managing a Sea of Information: Shipboard Command and Control in the United States Navy, 1899-1945," Ph.D. Dissertation, MIT Program in Science, Technology, and Society, 2003

mobility, and as armor and assembly lines increased mass, information problems for the control of all the above came to the fore. Clausewitz notes that "as operations become more and more fragmented, more diversified and specialized, the role of intelligence will in general have to increase."[5] Staff and intelligence organs flush with IT emerged to meet the increasing cognitive load of modern warfare.

By the Second World War the great powers had incorporated IT into a wide range of applications both traditional and novel: extensive radio and cable networks to direct far-flung ground and naval forces; ground-based and airborne radar to identify enemies and aid navigation beyond visible range; detailed aerial reconnaissance and photographic interpretation to guide and assess tactical operations and strategic bombing; the representation and control of submarine and merchant convoy activity across entire oceans; electromechanical cryptology and esoteric electronic warfare; standing cartographic bureaus, domestic population registries, and intelligence agencies; sprawling staff organizations to track and synthesize all this data; the first generation of in-flight maneuverable munitions; *etc.* World War II established the essential contours of modern "command and control" (C2), a term to describe the flow of mission-critical information throughout a distributed enterprise of people and machines.

During the Cold War, the acronym C2 became C3 with the appendage of "communications" and then C3I with "intelligence." IT networks ever more thoroughly innervated far-flung military forces, and they also enervated commanders who now had to pay more attention to breakdowns in their distributed cognitive systems. The C3I nervous system connected strategic decision-makers to early warning intelligence and to nuclear missiles, bombers, and submarines. Leaders expected to be able to control strategic nuclear forces even after a Soviet first strike in order to guarantee a reliable second strike deterrent and to exercise "escalation dominance" in the midst of a nuclear exchange. Critics, however, began to worry that C3I systems might be crippled by the electro-magnetic pulse of a nuclear blast, degradation by computer hackers, or the unintended consequences of organizational routines.[6] Such weaknesses might undermine U.S. strategic doctrine or, more ominously, cause conventional

---

[5] Clausewitz, *On War*, 349

[6] Bruce G. Blair, *Strategic Command and Control: Redefining the Nuclear Threat* (Washington, DC: Brookings Institution, 1985); Paul J. Bracken, *The Command and Control of Nuclear Forces* (New Haven, CT: Yale University Press, 1983)

coercion to inadvertently trigger a nuclear response.[7] Worries over strategic C3I survivability spurred the Defense Department to invest in the decentralized packet-switching communication protocols which underlie the modern internet.[8]

Conventional (non-nuclear) radio and computing systems were also plagued by vulnerabilities and incompatibilities. David Packard, co-founder of IT giant Hewlett-Packard and Deputy Secretary of Defense in the Nixon administration, championed the rationalization of C3I through an umbrella improvement program called the World Wide Military Command and Control System (WWMCCS). In a classic example of the collective action problems at the heart of enterprise IT, WWMCCS was hamstrung by interservice tussling: branches and units regularly defected from common coordination schemes to develop their own C3I systems.[9] Several high-profile communications failures such as radio glitches during the 1983 invasion of Granada amplified a growing drumbeat for defense reform. Not surprisingly, President Reagan's Blue Ribbon Commission on Defense, chaired by Packard, cited C3I interoperability as a major reason for centralization of the Department. The Packard Commission's recommendations formed the basis for the Goldwater-Nichols Act of 1986, which consolidated the authority of the Joint Staff and unified geographical and functional commanders over the individual services. Thus the most sweeping reform of the Department of Defense since its founding in 1947 was driven in no small part by worries over the growing IT intensiveness of the U.S. military.[10]

By the 1990s the term C3I had expanded into C4I with the addition of "computers" and ultimately C4ISR with "surveillance and reconnaissance." Some British writers included "target acquisition" for a more sonorous C4ISTAR. Bordering on the ridiculous, C5ISR/IO has even

---

[7] Barry R. Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks* (Ithaca, NY: Cornell University Press, 1992)

[8] Centralized exchanges, which predominated into the 1990s, might not function after destruction of portions of the network, whereas decentralized host-level routing could compensate for network damage as well as accommodate unplanned network growth. Nuclear survivability was not the only driver of the internet by any means, and in fact, the Advanced Research Projects Agency (ARPA) often used military justifications to rhetorically promote blue-sky research ventures. While funded with defense money, early internet engineers had wide latitude to follow their own interests. See Janet Abbate, *Inventing the Internet* (Cambirdge, MA: MIT Press, 2000). The early Office of Naval Research (ONR) similarly used the fig leaf of military application to justify basic research, as described by Harvey M. Sapolsky, *Science and the Navy: the History of the Office of Naval Research* (Princeton, NJ: Princeton University Press, 1990)

[9] David E. Pearson, *The World Wide Military Command and Control System: Evolution and Effectiveness* (Maxwell Air Force Base, AL: Air University Press, 2000)

[10] Kenneth C. Allard, *Command, Control, and the Common Defense* (New Haven, CT: Yale University Press, 1990)

made a recent appearance with the addition of "combat systems" and "information operations."[11] The term C4ISR has become a catchall category for the interdisciplinary application of IT to military operations of any sort: the production of fire and shock, maneuver of forces, operational planning and staff management, intelligence and reconnaissance, procurement and distribution of supplies, personnel training and administration, public affairs, and so forth.

The IT- and knowledge-intensiveness of military organizations has developed right along with the terms to describe it, from the moral and strategic problems of "command" to the more technical and tactical problems of C4ISR. This dissertation refocuses attention on the human problems at the heart of C4ISR and on the increasing prevalence of human-machine symbiosis in military cognition. Military knowledge management functions have become more nuanced and specialized over the past century, while at the same time they become more interconnected. From "command" to C2, C3, C3I, C4I, C4ISR, C5ISR/IO to who knows what next, military jargon strains to express this increasing differentiation and interdependence in a single term. The awkward agglutination raises the question, where is IT *not* involved in the military enterprise?

2.1.2 A Ubiquitous Technology

The U.S. military invests heavily in IT. The Department of Defense reportedly requested $43.3 billion for C4ISR across all categories of the 2011 budget, while C4ISR accounts for over 6% of the total budget.[12] Precise numbers are hard to estimate because so much IT falls within units' discretionary budgets, is included within the procurement and operating budgets of other items, or because some accounting categories have only appeared in recent years. In 2010 the U.S. Department of Defense had over 7,000 major applications on 7 million computers connected through 15,000 different networks, 21 satellite gateways, and 20,000 commercial circuits. 300,000 support personnel administered this sprawling tangle. While the capital costs

---

[11] *E.g.*, U.S. Naval Network Warfare Command, "Naval Network Warfare Command Strategic Plan 2009-2013," Version 4.0, 19 February 2009, http://www.netwarcom.navy.mil/about-us/StrategicPlan.pdf

[12] "Defense Funding for C4ISR Remains Stable," Defense Talk blog (23 June 2010), http://www.defencetalk.com/defense-funding-for-c4isr-remains-stable-27176/ (accessed 22 October 2010). This industry estimate takes into account C4ISR spending across different weapons programs and across research & development, procurement, and operations & maintenance budget. Only $5B or 4.5% of the FY2009 $112B Procurement budget is explicitly coded C4ISR, but a lot of IT spending is included in the procurement of ships, aircraft, munitions, *etc.*, not to mention administrative spending; Congressional Budget Office, "Long-Term Implications of the Fiscal Year 2010 Defense Budget," January 2010.

of computers declined by 80% in the previous two decades due to a thriving commercial market, the costs of defense network administration more than doubled in the same period.[13]

IT is ubiquitous in the workspaces and embedded in the weapon systems of all of the military services. Personnel use IT to perform the cognitive tasks of perceiving, planning, persuading, and communicating while robotic systems take on more of the burden of physical reconnaissance and the delivery of violence (the so-called "dull, dirty, or dangerous" jobs). A recent volume on the non-material sources of military effectiveness describes effectiveness as a function of military activities—strategic assessment, procurement, strategic and tactical C2, intelligence, internal monitoring, officer selection and assignment, training and education—which are themselves shaped by extra-military factors such as domestic economic strength, civil-military relations, national and international norms, *etc.*[14] Significantly, all of these "non-material" activities that influence military effectiveness are themselves thoroughly infused with IT. All involve gathering, processing, and communicating data via the manipulation of records, forms, databases, and displays. Ubiquitous IT plays a somewhat invisible but necessary role in the functional life of a military organization. Officers at all echelons cannot help but take an interest in their C4ISR architecture in their efforts to align organizational means and strategic ends. A technology which mediates perception is quite literally in the way.

The general-purpose nature of IT is one of its most striking features, not to mention a deliberate goal of computer engineers.[15] Microsoft *Excel* can run the accounts of an anti-war activist as well as an Air Force target list. Whereas previous technological innovations gave rise to new branches such as armor corps or carrier aviation, or even a whole new service in the case of the Air Force, by contrast militaries have incorporated IT into nearly *all* of their

---

[13] Paul A. Strassmann, "Information Dominance Bows to Network Limitations," *Signal Magazine* (Aug 2010). Similar numbers are reported by General Keith Alexander, Commander of U.S. Cyber Command and Director of the National Security Agency, in a talk entitled "U.S. Cybersecurity Policy and the Role of U.S. CYBERCOM" delivered at the Center for Strategic and International Studies (CSIS), Cybersecurity Policy Debate Series, 3 June 2010. http://csis.org/files/attachments/100603_alexander_transcript.pdf

[14] Risa Brooks and Elizabeth Stanley, ed., *Creating Military Power: The Sources of Military Effectiveness* (Stanford, CA: Stanford University Press, 2007) define the components of effectiveness as the integration of efforts, responsiveness to change, skill of personnel, and quality of material, which together contribute to military outcomes like victory, conflict duration, territorial gain, and casualties.

[15] Jon Agar, *The Government Machine: A Revolutionary History of the Computer* (Cambridge, MA: MIT Press, 2003) finds the roots of Allan Turing's mathematical idea of the universal computing machine in the British ideal of an apolitical, reliable, general-purpose civil service, in which Turing and his father both served in various capacities.

communities.[16] IT enables military outfits, whatever their functional specialization, to enhance the scope and precision of their administrative reach. Specialist communities have indeed emerged around IT—technical intelligence, computer network administration, psychological warfare—but they tend to be support communities parceled out to the combat arms rather than primary combat arms themselves (ambitions of modern day cyberwarriors notwithstanding).[17]

2.1.3 Knowledge Work

Morris Janowitz describes a long-term transformation in the nature of military authority from direct "domination" to indirect "manipulation."[18] He credits the shift from traditional authoritarian command to a more technocratic and collaborative style of management to the growing complexity, destructiveness, and automation of weaponry. At the bottom of the military hierarchy, the lethality of the modern battlefield makes close-order tactics suicidal and places a greater premium on small-unit initiative and inventiveness. At the top, military elites are concerned with policies shaping the procurement and employment of forces that both employ and affect large numbers of civilians.[19] In the middle, staffs expand to manage complex relationships within and across government agencies and with civilian science and technology firms. Janowitz argues that the result is the civilianization of the military, with greater leadership emphasis on negotiation, technical specialization, and efficiency improvement rather than domination in person on the battlefield. This administrative transition creates tension with traditional forms of warrior authority and with the residual need to ensure combat

---

[16] James W. Cortada, *The Digital Hand, Vol 3: How Computers Changed the Work of American Public Sector Industries* (New York, NY: Oxford University Press, 2008), 49-101, provides a detailed history of the U.S. Defense Department's voracious consumption of and dependence on IT from the 1940s through the 1990s. Cortada notes that the U.S. has tended to automate weapons and weapons platforms prior to administrative functions, which is consistent with the general military preference for offensive capabilities because they improve control, enhance autonomy, garner resources, and appeal to a warrior ethos. Yet even if this bias against administrative activities is allowed, IT has still been catholically applied to offensive applications across the board, rather than just one community.

[17] The recent emergence of an IT-only theory of victory and organizations to support it is discussed below in the section on cyber security.

[18] Morris Janowitz, "Changing Patterns of Organizational Authority: The Military Establishment," *Administrative Science Quarterly* vol. 3, no. 4 (1959): 473-493; Morris Janowitz, *The Professional Soldier: A Social and Political Portrait* (New York, NY: Free Press, 1960).

[19] Janowitz refers to nuclear deterrence, but the contemporary preoccupation with counterterrorism and state-building also admixes military and civilian interests.

effectiveness.[20] The civilianization of great power militaries has continued, if not accelerated, in the decades since Janowitz pointed it out.

This indirect style of management applies not only to authority relations in an organization, but also to the ways in which personnel control and experience the battlefield indirectly through IT. More personnel more of the time experience warfare through a computer screen. Even those who are still bodily exposed to combat nevertheless find themselves busied with computers before, after, and even during operations in the field. Rather than personally fighting in combat, they enable other people and machines to fight at some distance removed in space and time.[21] Instead of directing men and operating machines on the battlefield, officers manipulate email and *PowerPoint* slides and attend video teleconferences and staff meetings. Their workspaces resemble corporate office spaces anywhere.

These indirect IT-intensive jobs could be described as information, staff, office, or knowledge work.[22] This work is not simply clerical or administrative support, for it guides decisions on the use of force from the strategic to the tactical level. The emerging emphasis in war colleges and warfighting organizations on an intermediate "operational level of war" between theater strategy and battlefield tactics attests to the growing numbers of personnel who fight "war upon a map," as Jomini put it.[23] Ever more personnel and staff echelons perform

---

[20]Janowitz (*Ibid.*, 493) observes that "The movement from domination to manipulation seems to be a general pattern of social change. The fact that it is present even in the military is of particular theoretical importance." The military mission of physically destroying like kinds is so different from the mission of any other human organization, that if we see similar phenomena between them, it's a testament to how robust or universal such phenomena are.

[21] The difference between direct and indirect participation in combat can be likened to the cognitive difference between actions that change the world in order to reach a goal ("pragmatic" action), and actions that simplify the process of deciding what action to take ("epistemic" action), as described by David Kirsh and Paul Maglio, "On Distinguishing Epistemic From Pragmatic Action," *Cognitive Science* vol. 18, no. 4 (1994): 513-549. Wolters, "Managing a Sea of Information," 23, argues, "For American naval commanders in the first half of the twentieth century, the cognitive experience of command at sea increasingly shifted from one of pragmatic actions to one of epistemic actions."

[22] U. Schultze and R.J. Boland, "Knowledge Management Technology and the Reproduction of Knowledge Work Practices," *Journal of Strategic Information Systems* vol. 9 (2000): 193-212; Walter W. Powell and Kaisa Snellman, "The Knowledge Economy," *Annual Review of Sociology* vol. 30 (2004): 199-220; Greg Downey, "Virtual Webs, Physical Technologies, and Hidden Workers: The Spaces of Labor in Information Internetworks," *Technology and Culture* vol. 42, no. 2 (2001): 209-235; Heinrich Joachim Schwarz, "Techno-Territories: The Spatial, Technological and Social Reorganization of Office Work," Ph.D. Dissertation, MIT Program in Science, Technology and Society, 2003

[23] Antoine-Henri Jomini, *The Art of War*, trans. G. H. Mendell and W. P. Craighill (1862), Project Gutenberg Etext no. 13549 (28 September 2004), 69, describes the "grand tactics" of placing formations on the battlefield or

intermediate symbol-processing tasks in office cubicles, glittering command centers, and *PowerPoint* briefing sessions to indirectly guide the application of violence on the battlefield.

2.1.3.1 Officer-Enlisted Ratio

A traditional division of labor between information-processing management and physical labor is the officer-enlisted distinction. The ratio of officer to enlisted personnel has been steadily increasing over the past century, from 5% in 1900 to over 20% in 2000 (Figure 2-1).[24] This trend suggests greater emphasis on management and demand for college-educated personnel, as well as greater focus on leading smaller, more functionally differentiated work units rather than large masses of men. Enlisted personnel, furthermore, are increasingly likely to have college degrees. In many operational positions noncommissioned officers and junior officers actually perform the same work, as on intelligence watch floors where O-3s and E-7s often rotate through the same position.

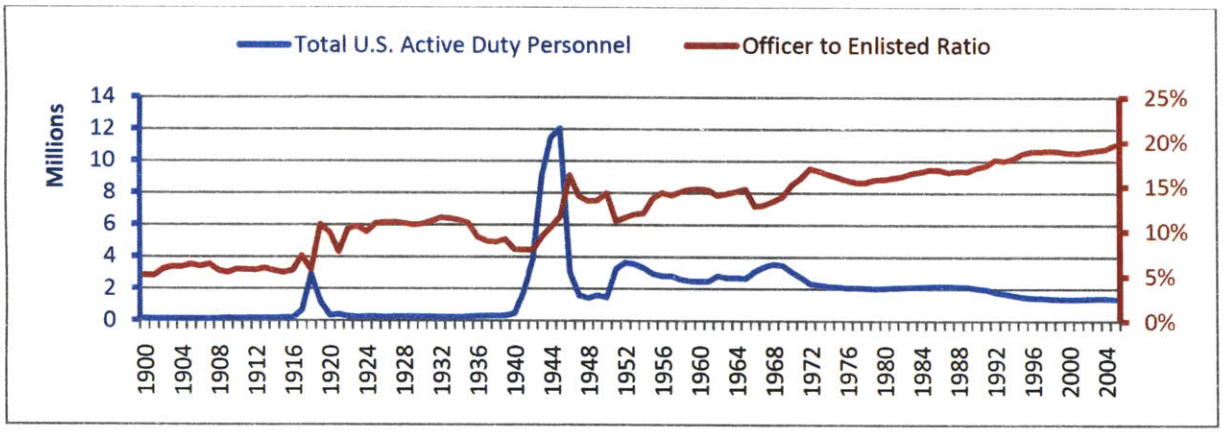


Figure 2-1: U.S. Officer-to-Enlisted Ratio 1900-2005

"planning upon the map." The "operational level of war" is that nether region of headquarters staffs which implement strategic objectives in a particular theater without getting dirty with tactical maneuvers. In practice this notoriously vague term can refer to a particular echelon like Multi-National Corps Iraq or a functional information-processing hub like a Combined Air Operations Center. However it's defined, the operational level is not quite theater strategy and not quite battlefield tactics, which seem more intuitively understandable, but an indirect mode of fighting "war upon the map" by directing, informing, and resupplying fielded forces. See Edward N. Luttwak, "The Operational Level of War," *International Security* vol. 5, no. 3 (1981): 61-79; Milan N. Vego, *Joint Operational Warfare: Theory and Practice* (Newport, RI: Naval War College, 2007).

[24] U.S. Department of Defense, "Selected Manpower Statistics, Fiscal Year 2005," Defense Manpower Data Center, 2005. Figure 2-1 shows that the ratio gets a bump after each major war, which suggests that more officers are retained during the overall drawdown. The 5% average prior to World War I is abnormally low, as the average throughout most of the 19th century, with the exception of the Civil War, is around 10%. Nonetheless, the rising ratio of officers in the long term is unmistakable.

2.1.3.2 Tooth-to-Tail

The line to staff or "tooth-to-tail" ratio, which measures personnel in combat-arms units like infantry and armor against those in headquarters, intelligence, and logistics units, has been steadily declining. The ratio has traditionally been comparatively lower in the American military than other states. The decline is more pronounced in maneuver units, which should be expected to have the bulk of Army combat power, than in expeditionary armies as a whole (Figure 2-2).[25] Whereas combat arms comprised 80% of a World War I division, less than 50% of a present day modular combined arms brigade consists of combat specialties. These figures do not capture the substantial amount of information processing that goes on *within* a combat unit. Organic intelligence and headquarters units have grown much larger and continue to expand; for example, the number of intelligence personnel at the battalion level tripled between 2003 and 2008.[26] Overall U.S. tooth-to-tail ratios have been declining, certainly more steeply than coarse functional measures indicate, as IT-intensive operations require more personnel to perform knowledge work instead of physical fighting roles.

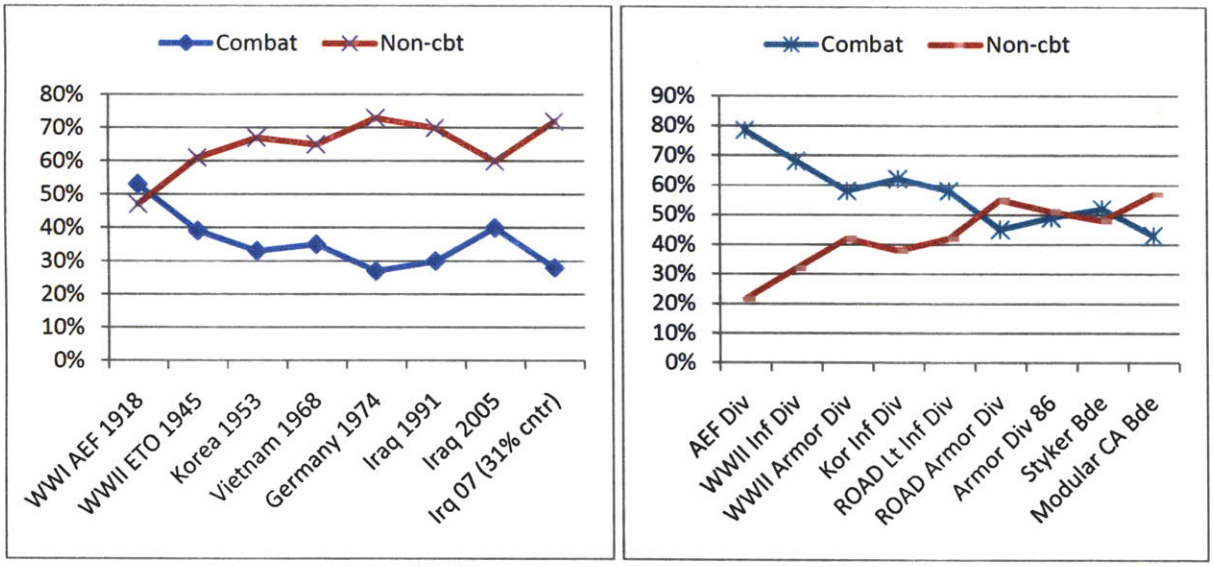


Figure 2-2: U.S. Army tooth-to-tail ratios in expeditionary armies and primary maneuver unit.

[25]John J. McGrath, "The Other End of the Spear: The Tooth-to- ail Ratio (T3R) in Modern Military Operations," Fort Leavenworth Combat Studies Institute, Long War Series Occasional Paper 23, 2007. The dip in 2005 on the left graph of Figure 2-2 is somewhat spurious as many of the non-combat positions had been replaced by contractors, which is why they are added back into the 2007 totals. 31% of the U.S. army deployed in Iraq in 2007 were civilian contractor personnel.

[26] Raymond T. Odierno, Nichoel E. Brooks and Francesco P. Mastracchio, "ISR Evolution in the Iraqi Theater," *Joint Forces Quarterly*, no. 50 (2008): 51-55

2.1.3.3 Occupational Specialties

In 2008 only 18% of U.S. enlisted personnel were in combat arms specialties, and only 36% of officers were in tactical operations (Table 2-1).[27] These statistics present an inflated sense of combat specialization. Officers rated for "tactical operations" also serve in command, staff and training billets. The enlisted ratings do not break out intelligence personnel, who may be coded as combat specialists in some cases. Many new information-focused occupational specialties have emerged and/or grown in recent decades: network administrators and computer technicians, intelligence (cryptology, espionage, interrogation, analysis, collection management), information operations (psychological warfare, propaganda, computer network attack and defense), space operations, meteorology, operations research, public affairs, and so forth. At the same time, personnel in traditional specialties also work with IT, intelligence, representation, and general information problems. The proliferation of service war colleges and emphasis on command and staff training also highlights the increasing importance of knowledge work across functional lines, not just in the formally designated information communities.

Table 2-1: U.S. military occupational specialties 2008

Enlisted Specializations (%)	
Combat	18.2
Electrical	20
Admin	15
Supply	10.3
Comms	9.7
Electronics	7.6
Medical	6.8
Non-occupational	5.9
Craftsman	3.5
Technical	3.3

Officer Specializations (%)	
Tactical Ops	36.3
Medical	17.3
Engineering	12.3
Supply	8.5
Non-occupational	7.11
Scientists	6.3
Admin	6.12
Intelligence	5.7
General/Flag	0.5

2.1.3.4 Civilian Contractors

Tooth-to-tail ratios based on military personnel alone significantly undercount the staff-intensiveness of organizations that employ a lot of contractors. In 2010 contractors made up 54% of the Defense Department workforce in Iraq and Afghanistan, and there were 19% more contractors than uniformed personnel in Iraq.[28] While the bulk of these were logistics jobs, there

[27] U.S. Department of Defense, "Population Representation in the Military Services, Fiscal Year 2008," Office of the Under Secretary of Defense, Personnel and Readiness, 2008

[28] Moshe Schwartz, "Department of Defense Contractors in Iraq and Afghanistan: Background and Analysis," Congressional Research Service, 2 July 2010

were also considerable numbers of contractors in IT support and intelligence analysis. 2.5 million civilian contractors joined the manpower roles in the Defense Department between 2002 and 2005, bringing the total number of federal employees and contractors to 14.6 million.[29] Hundreds of thousands of contractors work in intelligence, with 265,000 possessing a top secret clearance.[30] A clear symptom of the civilianization Janowitz notes is the presence of contractors and government civil servants working right alongside and often performing the same type of work as military intelligence, operations, and logistics personnel at their desks.

2.1.3.5 Sprawling Staffs

Military staffs are larger and more pervasive than ever. Empirical measurement of the expanding size and complexity of headquarters staffs is beyond my scope, but the essential trends are clear. The staffs of the U.S. Navy's deployed Fleets headquarters have become so large that, with the exception of U.S. 7th Fleet in the Western Pacific, they are no longer embarked on flagships.[31] Staff sections appear at even the lowest echelons, as with intelligence departments in Army and Marine companies, and even at the platoon level in the special operations community. Command staffs are also increasingly functionally differentiated, with dense interdependencies and cross-functional relationships. Many staff units sprawl across geographical boundaries. U.S. Central Command (CENTCOM), which runs the wars in Iraq and Afghanistan, is headquartered in Tampa, Florida. Predator drones, which conduct surveillance and targeted killings around the world, are piloted from Creech Air Force Base in Nevada. A proliferation of "reach back" intelligence organizations located in Washington D.C. and elsewhere in the continental U.S. provide tactical intelligence to deployed units. Complex staffs coordinate complex operations, but at the same time, staff complexity diffuses command responsibility and busies staffers with coordination problems and committee meetings. The institutions which arise to supply information-processing also create their own demand for it.

---

[29] Paul C. Light, "The New True Size of Government," Organizational Performance Initiative, Research Brief no. 2 (2006), http://wagner.nyu.edu/performance/files/True_Size.pdf. Light shows that the decline in the numbers of federal employees in the 1990s, publicized as a streamlining of government, was more than offset by expanding numbers of government contractors. The true size of government in the U.S. has long been on the increase.

[30] Dana Priest and William M. Arkin, "National Security Inc.," *Washington Post* (20 July 2010)

[31] In addition to the sheer numbers of people on number fleet staffs, IT is more reliable and bandwidth greater ashore to facilitate the type of network-centric command the Navy prefers.

2.2 Prophets of Information Dominance

The growth in knowledge intensiveness is a long term evolutionary development, not a recent saltation into "network-centric warfare" with the advent of the internet. The empirical trends sketched above—the emergence of new information specializations and changes in force structure, growing staff complexity, and intensive acquisition and staffing emphasis on C4ISR—are all circumstantial indicators of the growing knowledge-intensiveness of military organizations. Put simply, the military's brain has grown relatively larger and more complex. The emergence of RMA debate in the 1990s is more symptomatic of the growth of this trend past some threshold of awareness rather than a cause of pervasive computerization and networking. The articulation of doctrinal RMA concepts has surely intensified and abetted this trend, in part by providing marketing language for program offices and defense contractors. Nevertheless, expectations for better fighting through IT have a much earlier lineage.

2.2.1 The Modern Alexander

Not long after retiring as Chief of the German Imperial Staff in 1906, Field Marshall Alfred Graf von Schlieffen wrote an essay about modern warfare. He believed that emerging information technology (IT) would change the nature of military command:

> The warlord will be located farther in the rear, in a house with spacious offices, where wire and wireless, telephone, and signaling equipment are available. Hordes of lorries and motor vehicles, fitted out for the longest journeys, there await their marching orders. There, seated on a comfortable chair, in front of a large desk, the Modern Alexander will have the entire battlefield under his eyes on a map. From there he telephones inspiring words, receives the reports of army and corps commanders, captive balloons, and dirigibles, which all along the front watch the enemy's movements and register his positions.[32]

Schlieffen's essay anticipates many ideas about information-age warfare that would become popular in defense intellectual circles decades later. Translated into contemporary American military jargon, the "unblinking eye" of balloons and dirigible sensor networks provides "situational awareness" all along the front's "battlespace." Telephone, wireless, and signaling "data links" transmit information to a "reach-back" "joint operations center" with comfortable chairs, where officers in the rear resemble corporate managers more than battlefield

[32]Alfred Von Schlieffen, "Der Krieg in Der Gegenwart," *Deutsche Revue* vol. 34, no. 1 (1908): 13-24, p. 18. Translation by Martin Van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985), 153.

warlords. Spread out on the desk, a panoptic "common operational picture" enables the "joint forces commander" to direct "effects-based operations" via inspiring words and long-range, precision-guided lorries.

2.2.2 The Electronic Battlefield

Schlieffen's vision found fresh expression in the American military during the Vietnam War as the "electronic battlefield." General William Westmoreland, the U.S. Army Chief of Staff in October 1969, described the idea in a widely-cited address to the Association of the U.S. Army:

> On the battlefield of the future, enemy forces will be located, tracked, and targeted almost instantaneously through use of data links, computer assisted intelligence evaluation and automated fire control. With first round kill probabilities approaching certainty, and with surveillance devices that can continually track the enemy, the need for large forces to fix the opposition physically will be less important...[A]n improved communicative system...would permit commanders to be continually aware of the entire battlefield panorama down to squad and platoon level...With cooperative effort, no more than ten years should separate us from the automated battlefield.[33]

Schlieffen's balloons and dirigibles transmogrified into intelligence satellites and reconnaissance aircraft; headquarters maps became electronic displays of "the entire battlefield panorama"; and militaries would attempt to trade large and expensive forces in the field for "continually aware" commanders who enjoyed "probabilities approaching certainty." The American military, endowed with a robust industrial base and democratic constraints on taking casualties, has a long tradition of substituting firepower and technology for manpower.[34] The electronic battlefield concept carried this trend to an extreme, substituting IT for functions of the human mind and precise information for military mass. Advances in sensors, datalinks, and computational processing would provide more efficient collection, display, interpretation, and communication of information, and this would in turn lead to greater speed, precision, and economy in the management of violence. Robotic systems, furthermore, would make decisions

---

[33] Reprinted in Paul Dickson, *The Electronic Battlefield* (Bloomington, IN: Indiana University Press, 1976), 215-223

[34] Alex Roland, "Technology, Ground Warfare, and Strategy: The Paradox of the American Experience," *Journal of Military History*vol. 55, no. 4 (1994), 447-67; Russell F. Weigley, *The American Way of War: A History of United States Military Strategy and Policy* (Bloomington, IN: Indiana University Press, 1973)

faster than others and thus wage electronic warfare against one another.[35] A technology of the mind would also be a technology of control. Smarter forces would be able to do more with less.

2.2.3 Offset Strategy

While Westmoreland's ten-year timeline proved over-optimistic, his vision grew steadily more influential. By the mid-1970s hawkish observers believed that the Soviet Union had achieved parity with U.S. nuclear forces and that NATO conventional forces were outnumbered in Central Europe.[36] U.S. defense planners sought to redress the putative imbalance by compensating for Soviet advantages with advanced precision weapons and reconnaissance systems. In the mid-1980s NATO doctrinally codified the aptly-named American "offset strategy" as the Follow-on Forces Attack (FOFA) concept, a close relative of the U.S. Army's "AirLand Battle" doctrine. FOFA aimed to aggressively target Warsaw Pact forces that were expected to stream in from the East to exploit initial successes against NATO defenders.[37] The offset strategy relied on a dazzling array of weapons in the research and development pipeline, such as radar-evading stealth aircraft, laser-guided bombs, terrain-following cruise missiles, airborne moving target detection systems (JSTARS), and satellite constellations for communication, intelligence collection (DSP), and navigation (GPS). The U.S. Navy similarly pursued surveillance and targeting networks throughout the Cold War to facilitate over-the-horizon engagement of enemy aircraft and vessels as well as persistent monitoring of Soviet submarines.[38]

---

[35]Frank Barnaby, *The Automated Battlefield* (London: Sidgwick& Jackson, Ltd, 1986); Steven M. Shaker and Alan R. Wise, *War Without Men: Robots on the Future Battlefield* (Washington, DC: Pergamon-Brassey's, 1988)

[36] Calculation of the strategic balance turns on whether one counts warheads, launchers, throw weight, megatonage, *etc.*, so the numbers have been massaged to support various hawkish or dovish arguments. The conventional balance on the Central Front was often assumed to be a 3-to-1 advantage for the Pact over NATO, but *cf.* Barry R. Posen, "Is NATO Decisively Outnumbered?," *International Security* vol. 12, no. 4 (1988): 186-202, argues that when NATO command and logistics as well as Pact mobilization constraints are taken into account, local force ratios were effectively equal. Others argued that the Warsaw Pact's quantitative advantages were magnified by greater freedom of maneuver and depth in Eastern Europe compared to NATO in the West, as well as by American manpower limitations in the All-Volunteer Force, adopted after the trauma of draft mobilization for Vietnam.

[37]U.S. Congress, Office of Technology Assessment, "New Technology forNATO: Implementing Follow-On Force Attack," OTA-ISC-309 (Washington, DC: U.S. Government Printing Office, June 1987)

[38]Thomas G. Mahnken, *Technology and the American Way of War Since 1945* (New York, NY: Columbia University Press, 2008); Richard H. Van Atta, Michael J. Lippitz, Jasper C. Lupo, Rob Mahoney and Jack H. Nunn, "Transformation and Transition: DARPA's Role in Fostering an Emerging Revolution in Military Affairs," two vol., Institute For Defense Analyses Paper P-3698, 2003; Norman Friedman, *Seapower and Space: From the Dawn of the Missile Age to Net-Centric Warfare* (Annapolis, MD: Naval Institute Press, 2000)

Soviet observers like Marshal Nikolai Ogarkov viewed Western technical advances with growing alarm. Steeped in Marxist technological determinism, they wrote about an impending "military technical revolution" which was changing the mode of production of violence. As armored blitzkrieg had revolutionized land combat earlier in the century, they believed, so now electronic networks of sensors and guided weapons, which they called "reconnaissance-strike complexes," would determine the course of future conflicts. While the U.S. was further down the road with IT-intensive military modernization, the Soviets were perhaps thinking more systematically about the strategic implications. These Soviet ideas and fears entered American defense discourse largely through the efforts of Andrew Marshall in the Pentagon's Office of Net Assessment. Marshall encouraged U.S. planners to heighten Soviet fears by continuing to intensify the substitution of information and technology for manpower and mass in an economic race the Soviets couldn't hope to win.[39]

2.2.4 The Revolution in Military Affairs

Marshall's ideas found a wide audience in the 1990s, which were a perfect storm for military futurology. The vigorous infusion of IT into both nuclear and conventional operations—promising speed and accuracy for the offense while creating looming vulnerabilities for the defense and interoperability challenges—provided grist for excited claims about an information-age transformation of warfare. The end of the Cold War, the decisive defeat of Iraq in 1991, the rapid expansion of the internet and domestic IT industry, the globalization of industry and the media, popular hype over a brave new world of increasing returns to e-business, and the turn of the millennium all combined to give rise to prophesy of tectonic shifts in military power. Neologisms such as InfoWar, NetWar, FutureWar, and CyberWar emerged in popular discussions, breathlessly describing how technical developments would dramatically bolster or undermine American military prowess.[40] A book-length survey of the copious prognostication

---

[39] Dima P. Adamsky, "Through the Looking Glass: The Soviet Military-Technical Revolution and the American Revolution in Military Affairs," *Journal of Strategic Studies* vol. 31, no. 2 (2008): 257-294; Notra Trulock, Kerry Hines and Anne Herr, "Soviet Military Thought in Transition: Implications for the Long-Term Military Competition," Pacific-Siera Research Corporation Report No. 1831, May 1988; Andrew F. Krepinevich, Jr., *The Military-Technical Revolution: A Preliminary Assessment* (Washington, DC: Center For Strategic and Budgetary Assessments, 2002).

[40] Some of the more ebullient popular titles include: Alvin Toffler and Heidi Toffler, *War and Anti-War: Survival At the Dawn of the 21st Century* (Boston, MA: Little, Brown and Co, 1993); George Friedman and Meredith Friedman, *The Future of War: Power, Technology, and American World Dominance in the 21st Century* (New York, NY: Crown, 1996), John Arquilla and David F. Ronfeldt, *In Athena's Camp: Preparing For Conflict in the Information Age* (Santa

in the 1990s notes many disagreements over: whether the 1991 Gulf War was the first new war of the information age or the last old war between conventional militaries; whether the future portended more terrorism from newly-empowered actors or more great-power conflict; whether information age advances were accruing faster to the U.S. or its adversaries; whether the most important new capabilities were networks, robots, nanotechnology, or weapons of mass destruction; and overall, whether we should be hopeful or fearful.[41] Most futurists shared the assumptions that (1) the Cold War was an outmoded model of industrial age conflict, and (2) something radically new and more dangerous than superpower nuclear holocaust (one wonders) was emerging because of new technologies and globalization. They neatly divided the history of warfare into different eras, assuming that in the immediate future some of the old rules would no longer apply. Just as the economics of bricks-and-mortar business were supposedly altered for the new internet economy, so would IT usher in a radical new era of warfare.

In the midst of this futurist foment, Marshall's office released a well-timed and influential net assessment in 1992 which sought to generalize on the Soviet "Military-Technical Revolution" concept. Marshall organized panels and funded academic research to explain how changes in the technology of war, in general, create military advantage. He later reflected, "The effort yielded what seemed to be a consensus that we were in a period of major change; in short, that the Russian theorists were right. We also concluded from military history that changes of the scale that we were talking about would involve new concepts of operation, and new organizational structures and processes to execute these concepts."[42] Marshall's camp considered the 1990s to be especially analogous to the 1920s and 1930s as a period in which a major great power war had ended and militaries were scrambling to understand how emerging

---

Monica, CA: RAND, 1997); James Adams, *The Next World War: The Weapons and Warriors of the New Battlefields of Cyberspace* (London: Arrow, 1998), *etc.*

[41]Tim Benbow, *The Magic Bullet? Understanding the Revolution in Military Affairs* (London: Brassey's, 2004). The British author notes that the RMA debate is a peculiarly American obsession. In parsing the debate differently he identifies *radicals* who believed the RMA was underway with reconnaissance-strike complexes; *visionaries* who believed the RMA was yet to come with a whole new paradigm of techno-bestiaries; *skeptics* who believed that the RMA was just bureaucratic salesmanship; *moderates* who believed that RMAs might have happened in the past but the current changes didn't qualify; and *pessimists* who believed that the RMA was happening but that its changes were counterproductive for the west. My account focuses on Benbow's *radical* version of the RMA since that is the one that has been doctrinally embraced in the U.S. military, and then reviews the various criticisms that has been leveled at it.

[42]Krepinevich, "The Military-Technical Revolution," ii. On Marshall's role in promoting the RMA see Jason Vest, "The Dubious Genius of Andrew Marshall," *The American Prospect*, 15 February 2001, http://www.prospect.org/cs/articles?article=the_dubious_genius_of_andrew_marshall

technologies—armored tanks, strategic bombers, carrier aviation, submarines, and electronic warfare—would be used for next big conflict.[43] Those militaries which developed the best doctrinal concepts and organizational capacity to exploit the technology in peacetime, under this interpretation, naturally outperformed the rest in wartime.[44] The implication was that if the U.S. did not understand *and adapt to the inherent nature* of the IT revolution, then America might irreversibly slide behind a rising China or a resurgent Russia which did make the jump.

To emphasize the importance of getting the doctrine and organization right, Marshall rebranded the Soviet "Military-Technical Revolution" the "Revolution in Military Affairs." This rhetorical move parried charges of technological determinism by inserting a necessary organizational intervention: visionaries had to get the doctrine right and seduce the bureaucracy into accepting it during peacetime. Nevertheless, the RMA interpretation still assumed that IT inherently held certain potentials for business and military success if organizations could reorganize to exploit them, or else get left behind.[45] The war-winning potential of technology could only be held back by hidebound conservatism, which either ignored the technology or simply did familiar things with new tools.[46] The study of different RMAs throughout history—from "cavalry to computer" in one oft-cited article[47]—became something of a cottage industry. The term "RMA" proper usually refers to the most recent IT revolution. If IT was changing the world, then the US military had to change with it.[48]

---

[43]Williamson Murray and Allan R. Millett, *Military Innovation in the Interwar Period* (Cambridge University Press, 1996)

[44] Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca, NY: Cornell University Press, 1991), develops this theory of military innovation.

[45] Langdon Winner, *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought* (Cambridge, MA: MIT Press, 1977), discusses the historical fallacy and rhetorical usefulness of the idea that technology is an inexorably advancing force to which people must adapt.

[46] The classic study by I. B. Holley, *Ideas and Weapons* (New Haven, CT: Yale University Press, 1953), shows that there is a strong element of truth to this interpretation, but just because a bureaucracy fails to develop new doctrine for a technology does not mean that that technology necessarily favors a particular doctrine. Holley shows that the early adoption of aviation by the U.S. Army Signal Corps for observation hindered the development of fighter and bomber aircraft in World War I because there was no agreed doctrine on air power to guide the procurement and employment of the new weapons. This does *not* mean, however, that strategic bombing was the "right" doctrine for air power, as later frustrations with it in World War II would suggest.

[47] Andrew F. Krepinevich, Jr., "Cavalry to Computer: The Pattern of Military Revolutions," *National Interest* vol. 37 (1994): 30-42

[48]Eliot A. Cohen, "A Revolution in Warfare," *Foreign Affairs* vol. 75, no. 2 (1996): 37-54

2.2.4.1 Dominant Battlespace Knowledge

The basic features usually associated with the RMA are long-range precision strike, global intelligence networks, and heightened information sharing among services and combatants.[49] Put simply, reconnaissance-strike complexes with a heavy dose of "Jointness." Admiral William Owens, Vice Chairman of the U.S. Joint Chiefs of Staff in 1996, described an emerging "system of systems" which would "infuse DBK into all our forces [that is, dominant battlespace knowledge]" to realize the RMA's potential.[50] Owens' book *Lifting the Fog of War* articulated the most explicit version yet of the information-for-mass substitution strategy anticipated by Schlieffen and Westmoreland:

> I believe the technology that is available to the U.S. military today and now in development can revolutionize the way we conduct military operations. That technology can give us the ability to see a "battlefield" as large as Iraq or Korea—an area 200 miles on a side—with unprecedented fidelity, comprehension, and timeliness; by night or day, in any kind of weather, all the time. In a future conflict, that means an Army corps commander in his field headquarters will have instant access to a live, three-dimensional image of the entire battlefield displayed on a computer screen, an image generated by a network of sensors including satellites, unmanned aerial vehicles, reconnaissance aircraft, and special operations soldiers on the ground. The commander will know the precise location and activity of enemy units—even those attempting to cloak their movements by operating at night or in poor weather, or by hiding behind mountains or under trees. He will also have instant access to information about the U.S. military force and its movements, enabling him to direct nearly instantaneous air strikes, artillery fire, and infantry assaults, thwarting any attempt by the enemy to launch its own attack. And the same powerful computer networks that make this possible will also grant the U.S. commander the ability to streamline the historically cumbersome supply process, making the whole force more mobile and therefore less vulnerable to attack.[51]

---

[49]Barry D. Watts, "Six Decades of Guided Munitions and Battle Networks: Progress and Prospects," Center for Strategic and Budgetary Assessments, March 2007; Paul G. Gillespie, *Weapons of Choice: The Development of Precision Guided Munitions* (University Alabama Press, 2006)

[50]William A. Owens, "The Emerging U.S. System-of-Systems," *National Defense University Strategic Forum* No. 63 (1996)

[51] William A. Owens with Edward Offley, *Lifting the Fog of War* (New York, NY: Farrar, Straus and Giroux, 2000), 15-16. This title has also been used in other articles anticipating the ability of computers to control uncertainty in war, *e.g.*: Eric C. Ludvigsen, "Lifting the Fog of War," *Army* (July 1972); Richard H. Buenneke, Jr., "Lifting the Fog of War," *Government Executive* (February 1991)

Owens pushed IT as an epistemic performance enhancing drug to overcome the confusion which had reigned throughout history on battlefields of 200 square miles or of any size. Clausewitz writes, "War is the realm of uncertainty; three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty. A sensitive and discriminating judgment is called for; a skilled intelligence to scent out the truth."[52] Owens essentially claimed that robust networking and Joint management would automate some of this judgment and intelligence. Rather than the situated intuition and pragmatic skill in the Clausewitzian account, knowledge became an objective substance that would "infuse" into forces. IT and Joint doctrine were to accomplish this feat by enabling organizations to make decisions faster than adversaries, or, in the coinage of Air Force test pilot John Boyd, to more rapidly run the "OODA loop" (observe, orient, decide, act).[53] The entire networked Joint force would "turn inside the decision cycle" of the enemy, just like a single fighter in a dogfight should outthink and outmaneuver his opponent. Boyd's conflation of tactical and strategic decision-making processes went largely unremarked in the RMA appropriation of the concept.

2.2.4.2 Joint Vision

Owens was a driving force in codifying the RMA into official U.S. doctrine. *Joint Vision 2010*, published in 1996, declared in its first sentence that it was "the conceptual template for how America's Armed Forces will channel the vitality and innovation of our people and leverage technological opportunities to achieve new levels of effectiveness in joint warfighting."[54] The document attempted to balance the Pentagon's internal debate over the RMA, which pitted traditional defenders of the central human element in war versus visionaries of the game-changing potential of emerging IT. This debate often broke out along service lines, with the manpower-oriented Army and Marines versus the more technophilic Navy and Air Force. Both sides could agree on the need to enhance "Jointness"—the Joint Staff management of interdependence, interoperation, and system procurement—even though they had different reasons: Joint management favored the unity of command long sought by the Army and now mandated by the Goldwater-Nichols reform; RMA advocates thought Jointness was necessary

---

[52]Carl von Clausewitz, *On War*, ed. and trans. by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1984), 101.
[53]Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (Boston, MA: Little, Brown and Co, 2002)
[54]U.S. Chairman of the Joint Chiefs of Staff, *Joint Vision 2010* (Washington DC: U.S. Government Printing Office, 1996), 1.

for gaining "information dominance" over current and emerging adversaries. The document stated that "increased access to information and improvements in the speed and accuracy of prioritizing and transferring data brought about by advances in technology" would enable information dominance, to which was added to placate critics, "While the friction and the fog of war can never be eliminated, new technology promises to mitigate their impact."[55] *Joint Vision 2020* followed in 2000, further reinforcing the drive to field information-age forces that "are to be faster, more lethal, and more precise in 2020 than they are today."[56]

2.2.4.3 Network Centric Warfare

The new doctrine further incorporated the ideas of yet another Navy admiral who, like Owens, had been influenced by the heady information-age excitement of the 1990s.[57] Vice Admiral Arthur Cebrowski, the Joint Staff director of command, control, and communications during Owens' tenure, introduced "network centric warfare" in an influential 1998 article.[58] He drew an explicit analogy between a supposed "Revolution in Business Affairs" and the RMA: "nations make war the same way they make wealth." In this story firms like Walmart and Fed-Ex embraced IT and flattened their organizations to become globally competitive, and so too would networked militaries thus win decisive victory. Cebrowski lambasted outdated "platform centric" ways of fielding expensive vehicles with top-down control, and instead advocated bottom-up "network centric" collaboration among a distributed array of "sensors and shooters." Whereas "situational awareness" supposedly deteriorated for platform-centric militaries as they were damaged in combat, the devolution of control to the "network edges" would "self-synchronize" awareness and "lock out" opponents. By cycling the "OODA loop" so rapidly that "it appears to disappear," the episodic nature of war emphasized by Clausewitz would merge into an omniscient and unrelenting knock-out blow.

---

[55] *JV2010*, 16.

[56] U.S. Chairman of the Joint Chiefs of Staff, *Joint Vision 2020* (Washington DC: U.S. Government Printing Office, 2000), 1

[57] On information-age discourse in general see Vincent Mosco, *The Digital Sublime: Myth, Power, and Cyberspace* (Cambridge, MA: MIT Press, 2004). Mosco places enthusiasm for cyberspace in a long tradition of American technological progressivism, described by David E. Nye, *American Technological Sublime* (Cambridge, MA: MIT Press, 1996)

[58] Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," *U.S. Naval Institute Proceedings* vol. 124, no. 1 (1998). Garstka also coauthored a book on NCW published by the Defense Department's C4ISR Cooperative Research Program (CCRP): David S. Alberts, John J. Garstka and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (Washington D.C.: CCRP Publications Series, 1999).

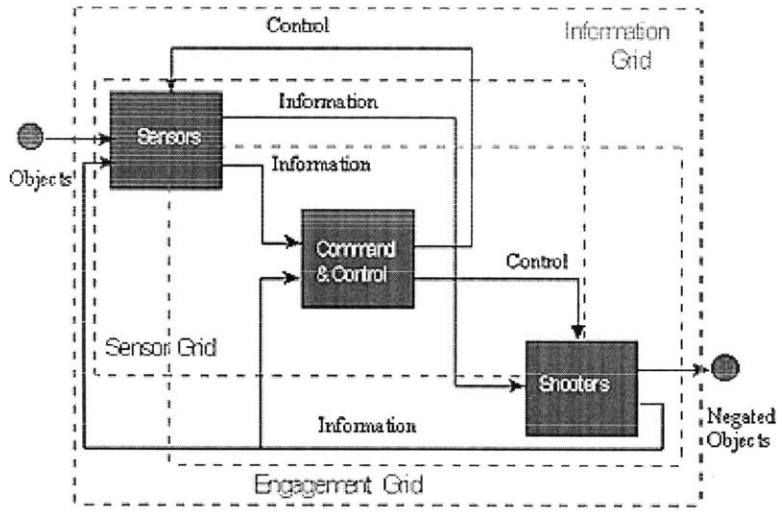


Figure 2-3: Cebrowski and Garstka's "Logical Model for Network-Centric Warfare"[59]

A diagram in the article (Figure 2-3) illustrated interlaced "grids" transforming "objects" into "negated objects," with no mention of the enemy's will or the miserable confusion of war. Just as corporate supply chains became more complex and disaggregated through globalization, so too the "kill chain"—which moves information from "sensors to shooter"—would become more robustly networked and responsive.

2.2.4.4 Defense Transformation

Cebrowski retired from the Navy after a final tour as president of the Naval War College, where he championed a vision of fast, cheap, networked "streetfighter" surface combatants.[60] In October 2001 he joined the George W. Bush administration as the civilian head of the newly-created Office of Force Transformation. Net-centric warfare provided the ideological aegis for Defense Secretary Donald Rumsfeld's aggressive agenda for "Transformation" of the Department. Cebrowski's job was to amass evidence and enthusiasm for the doctrine which justified the reforms.[61] If the only thing standing between the U.S. military and its information age destiny was a recalcitrant "platform centric" bureaucracy, then Rumsfeld resolved to

---

[59] Diagram from Cebrowski and Garstka, "Network Centric Warfare"

[60] Ironically, this concept has now been realized as the large, expensive, capability-laden, and decidedly platform-centric Littoral Combat Ship (LCS), of which the U.S. will produce decidedly fewer hulls than fighters in a modest street gang.

[61] Donald H. Rumsfeld, "Transforming the Military," *Foreign Affairs* vol. 81, no. 3 (2002); James R. Blaker, *Transforming Military Force: The Legacy of Arthur Cebrowski and Network Centric Warfare* (Westport, CT: Praeger, 2007)

overhaul outdated processes and attitudes in order to create a lighter, faster, networked force that could do more with less. Net-centricity was the goal of transformation, which the RMA required: as Cebrowski put it, "How Can the Military Not Change?"[62]

The Office of Force Transformation acted upon Andy Marshall's belief that intellectual concepts drove the institutionalization of new technology and doctrine. If such consensus-building had been somewhat *ad hoc* in previous historical RMAs, then Cebrowski's office would now deliberately construct the official intellectual foundation for Rumsfeld's aggressive agenda. Much like Marshall's Office of Net Assessment, Cebrowski's new office channeled funds to stimulate research into military innovation and information age operations. Its affiliated C4ISR Cooperative Research Program (CCRP) also self-published a number of books in order to build up a self-referential literature and jargon on information-age military operations.[63] The RMA was thus not only a military reflection of information-age hype, nor simply a spontaneous expression of the eternal quest for military control, but also the product of a deliberately constructed engine of intellectual consensus. Authors could cite the body of ideas produced through Cebrowski and Marshall's auspices, and defense contractors would be rewarded by including net-centric jargon in promotional materials.[64]

"Defense transformation" was the high-water mark of the doctrinal RMA, marking its institutionalization into the defense establishment.[65] As the U.S. became bogged down in a protracted insurgency in Iraq after 2003, the futurist dream dimmed a bit. Rumsfeld was replaced in the second Bush term, and the Office of Force Transformation was disestablished

---

[62]Cebrowski and Garstka, "Network-Centric Warfare"

[63] David Alberts, the lead author with Garstka on the first NCW book (n. 58 above), co-authored many of these CCRP titles. Alberts, like Cebrowski and most NCW enthusiasts, came from a computer engineering and operations research background, and he served as a senior officer with the MITRE corporation, a Federally-Funded Research and Development Corporation focused on C4ISR. Other notable CCRP titles published and promulgated in order to war colleges to build momentum for NCW include: David S. Alberts, John J. Garstka, Richard E. Hayes and David A. Signori, *Understanding Information Age Warfare* (Washington D.C.: CCRP Publications Series, 2001); David S. Alberts and Richard E. Hayes, *Power to the Edge: Command...Control...in the Information Age* (Washington D.C.: CCRP Publications Series, 2003); Edward A. Smith, *Effects Based Operations* (Washington D.C.: CCRP Publications Series, 2003)

[64] A critical intellectual history of the deliberate efforts to promote consensus about RMA and NCW has yet to be written. Key actors in the generation of futurist doctrine include Marshall's Office of Net Assessment, Cebrowski's Office of Force Transformation, the DoD C4ISR Cooperative Research Program, the National Defense University, and U.S. Joint Forces Command.

[65]Frederick Kagan, *Finding the Target: The Transformation of American Military Policy* (New York, NY: Encounter Books, 2006) provides a critical history of DoD Transformation policy

after Cebrowski passed away in 2005 following a long battle with cancer. Nevertheless, net-centric concepts and jargon had by then become ingrained in defense industry and military discourse (sometimes repackaged as the more anodyne "network-enabled operations" for European allies). Network-centric warfare came to refer, like C3I and C4ISR before it, to just about any military activity that involved IT networks, which seemed like more and more every year. The revolution was normalized.

2.2.5 Centralized Decentralization

Cebrowski's office promulgated four "tenets of NCW" which state the conventional wisdom in the C4ISR community. Expressed as a series of causal hypotheses, they can be taken together as an RMA theory of victory: (1) a robustly networked force improves information sharing and collaboration, (2) which enhance the quality of information and shared situational awareness, (3) which enables self-synchronization among pervasive sensors and long-range precision shooters, (4) which dramatically increase mission effectiveness (shorter duration, fewer casualties, and more decisive).[66] "Robustly networked" means interoperable systems, shared protocols, common data definitions, collaborative concepts, strong information security measures, and rationally integrated program management. The laissez-faire "self-synchronization" of networked forces is thus predicated on coordinated "Joint" management. In essence the RMA theory says that it's necessary to centralize in order to decentralize.

A charitable way to interpret this apparent contradiction is in terms of the basic political-economy insight that regulatory institutions are required for the efficient functioning of markets. Interconnected markets can be innovative and responsive, but without defined property rights and contract enforcement mechanisms, markets are vulnerable to failures like pollution externalities, bubbles and crashes, and unfair competition. Unfortunately, governmental regulators are vulnerable to other failures like policy capture, rent-seeking, and bureaucratic inefficiency. This interpretation points to the political problems at the heart of the RMA vision. RMA doctrine expects simultaneously for IT to empower the Modern Alexander in a comfortable staff headquarters as well as a chaotic swarm of streetfighters. Unfortunately, the parallel pursuit of centralized reliability and decentralized agility also invites the characteristic pathologies of both governments and markets. Information friction theory, developed in

[66] http://www.dodccrp.org/html4/research_ncw.html, accessed 2 March 2010. I added "pervasive sensors and long-range precision shooters," which is obviously part of the RMA vision but not part of these "tenets."

Chapters 3 and 4, develops these ideas to explain how real military information systems diverge from the technocratic RMA ideal. The rest of this chapter will take up the policy and academic challenges to RMA doctrine.

2.3 Criticisms and Reality Checks

Spanning a century of different technological possibilities and strategic problems, Schlieffen, Westmoreland, and Owens articulate a remarkably consistent vision of better knowledge and control through IT. Yet all of their contemporary militaries fell remarkably short of their ideals. Schlieffen's name is indelibly associated with the German plan for speedy victory over France in World War I, which degenerated into traumatic stalemate in the trenches.[67] Westmoreland is better known for Pollyannaish forecasts of progress during the buildup of American combat forces in Vietnam, a war plagued by failures to understand and adapt to the problems of irregular war. Owens' prediction of transparency in "a battlefield as large as Iraq" seems especially ironic in that only three years later, irregular foes in that country proved able to frustrate American technology for years.

Military officers often look to IT to improve control over war, but uncertainty, confusion, and brutal slogging have regularly confounded expectations. As the technological state-of-the-art advances and as novel military problems emerge, transformative IT-enabled solutions continually appear on the horizon. [68] Anthony Oettinger, founder of Harvard's Program on Information Resources Policy, describes a cyclic "ecstasy" of technological possibility and "agony" of implementation that falls short of the mark.[69] The agony of miscalculation and confusion is quite literal in war, and so many critics view the recurrent ecstasy of expectation

---

[67] The exact relationship between Schlieffen's 1905 staff paper and Moltke's actual invasion has recently generated some historiographical controversy; see Keir A. Lieber, "The New History of World War I and What it Means for International Relations Theory," *International Security* vol. 32, no. 2 (2007): 155-191.

[68] A century after Schlieffen and a decade after Owens, former Air Force deputy chief of staff for intelligence, surveillance, and reconnaissance (ISR) Lt. Gen. Dave Deptula expresses some familiar sentiments: "We stand at the cusp of a new era in military operations in which the speed of information, advancements in technology, networking of our organizations, and mind-set of our people will directly shape the success or failure of our future military activities. The foundations of our achievement will hinge on the ability to sense, know, decide, and act ahead of our adversaries on a global scale. These technologies and challenges have trumped the buffer of geography that historically afforded us the luxury of time to think and act, demanding that we alter our ISR farmer-culture mind-set and begin to act more like hunters." Dave Deptula and Mike Francisco, "Air Force ISR Operations: Hunting Versus Gathering," *Air & Space Power Journal* (Winter 2010): 13-17.

[69] Anthony G. Oettinger, "Telling Ripe from Hype in Multimedia: The Ecstasy and the Agony" in *The Information Resources Policy Handbook: Research For the Information Age*, ed. Benjamin M. Compaine, and William H. Read (Cambridge, MA: MIT Press, 1999), 3-28

with a jaundiced eye. IT does not always improve perception and control, and can in fact create dangerous misperceptions and vulnerabilities.

2.3.1 Vulnerable to Cyberattack

The first criticism of the RMA is actually just an extension of it. As militaries have incorporated electronic IT into their operations since the early 20th century, they have simultaneously developed ways to attack their adversaries' use of it by eavesdropping on, jamming, or spoofing their signals.[70] "Electronic warfare" traditionally focused on exploitation of the electromagnetic spectrum, but having been incorporated into "information operations" in Pentagon jargon, it increasingly includes hacking into computer networks to manipulate data and market messages.[71] Concern for cybersecurity is a natural consequence of conflict among RMA-enabled forces, which should be expected to attack one another's critical networks and vital data. Vulnerability to electronic attack and espionage has long been recognized as a liability of increasing dependence on IT, as discussed above in the concerns over nuclear C3I in the 1970s and 1980s. Moreover, the strong emphasis on "Jointness" in architectural standards stems in no small part from a desire to harden net-centric systems against cyber exploitation: thus "information assurance," "operational security," and "robustness" are often described as necessary traits of C4ISR systems in RMA doctrine.

Given the pervasiveness of IT in societal and military "critical infrastructure," some ambitious futurists envision a more exclusive role for IT in war: cyberwarriors could infiltrate networks to disable military capabilities and paralyze societal infrastructures without firing a

---

[70] Alfred Price, *The History of US Electronic Warfare*, 3 vols (Arlington, VA: Association of Old Crows, 1984, 1987, 2000)

[71] "Information Operations" is another catchall term in U.S. doctrine. Much like C4ISR, IO seems to include anything that might be done with information in the military via computers or humans (which excludes what?). In practice the term has two distinctly different connotations depending on service orientation. The Army and Marine Corps, with their focus on influencing humans on the ground, emphasize propaganda, marketing, and deception; IO has to do with delivering a message to a target audience. The more technologically-oriented Navy and Air Force emphasize attacks on electronic systems; IO has to do with manipulating the systems which deliver messages. The "five pillars" of IO are psychological operations (propaganda, marketing, influence), military deception (ruses and misleading information), computer network operations (attack through hacking), electronic warfare (attack through jamming and spoofing), and operational security (defense from enemy IO or information assurance); see U.S. Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations* (Washington, DC: Government Printing Office, 2006). The umbrella concept is so broad that it's hard to distinguish the emphasis on synchronized effects from the basic coordinating role of any bureaucratic staff; indeed, the prevalent usage of IO, like C4ISR, is another indirect indication of the growing importance of staffwork in everyday military operations.

shot.[72] Someday the U.S. could experience a "digital Pearl Harbor" and be unable to respond to it. The elaboration of cybersecurity ideas parallels the emergence of airpower in two ways. First, airplanes were originally used in support roles for observation or later as "flying artillery" before an exclusive airpower concept of strategic bombing was developed and dedicated organizations formed around the new technology.[73] While this dissertation emphasizes the catholic appropriation of IT across military communities as a complement to almost every functional area, rather than the emergence of exclusive IT warfighting communities, the cyberwar movement of the RMA is a major exception. Personnel in the recently-created U.S. Cyber Command, 24th Air Force, and U.S. 10th Fleet will ride only their mice into battle. Second, classic strategic bombing doctrine envisioned bypassing the battlefield altogether in order to directly attack the enemy's nerve centers, thus breaking his will to fight and/or his ability to command and control his forces.[74] Cyberwar could be described as "non-lethal strategic bombing" because it seeks to bypass direct military confrontation by exploiting military and civilian dependence on IT networks.[75] This capability supposedly empowers weaker states and non-state actors who might use IT to gain an asymmetric advantage over powerful militaries. The RMA makes great powers highly-dependent on IT, the argument goes, and thus highly-vulnerable to devastating cyber-attack: "the U.S. military is more vulnerable to cyber attack than any other military."[76] Furthermore, there's supposedly little that the Defense Department can do about it because IT infrastructures are largely owned and operated by private commercial actors who neither publicize their vulnerabilities nor invest in sufficient defense.

---

[72] The cyberwar literature is large and wooly. See for example, James Adams, *The Next World War: The Weapons and Warriors of the New Battlefields of Cyberspace* (London: Arrow, 1998), or more recently, Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York, NY: Harpercollins, 2010).

[73] Holley, *Ideas and Weapons*

[74] Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1996); Tony Mason, *Air Power: A Centennial Appraisal* (London, Brassy's, 1994)

[75] Owen R. Cote, Jr. coined the phrase "non-lethal strategic bombing." The air power theory of victory through strategic bombing alone has proven historically suspect because targets often find surprising ways to compensate for the effects of bombing and because airpower is more effectively employed as a complement to other combat arms. Thus one wonders how its defects might be repaired simply through the use of indirect, non-lethal means.

[76] Clarke and Knake, *Cyber War*, 225-6

Further discussion of cybersecurity is well beyond the scope of this project to assess.[77] Here I only want to emphasize that cybersecurity is just the contemporary embodiment and inverse image of traditional RMA concepts reviewed above. Cybersecurity and net-centric warfare share many of the same assumptions, the most important of which is that IT is remaking the world and so organizations must adapt or perish. Both assume that IT grants a high degree of knowledge and control which facilitates offense: network-centric forces can overwhelm their adversaries' decision cycles, and cyberwarriors can identify and interdict their adversaries' electronic pressure points to paralyze them.[78] Ideas of reconnaissance-strike complexes on the one hand and electronic warfare in cyberspace on the other have common roots and usually common champions in the C4ISR and information operations communities.[79] Fears about "cybersecurity" as the Achilles heel of networked militaries overstate the potential for cyber-catastrophe as much as net-centric warfare overstates the potential for rapid victory.

2.3.2 Not a Revolution

Historians and political scientists have identified multiple previous episodes of major military innovation which not only provide comparative context for understanding the IT RMA,

---

[77] The strategic import of cyberspace remains relatively undeveloped, in part because the engineering field of computer security has been conflated with the problems of international security. The former has borrowed a great deal of language from the latter to metaphorically describe hacker attack and defense, and this often has the result of overwhelming analysis of strategy with the esoteric complexity of tactical technical detail. Cybercrime and cyberespionage are probably the more serious, likely, and realistic problems, while cyberwarfare against critical infrastructure receives more excited rhetorical attention; the former two depend on the continuing integrity of networks while the latter aims to degrade them, which makes a big difference. The best treatments of cyberspace to date are Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge: MIT Press, 2001); Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge University Press, 2007); Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington DC: National Defense University Press, 2009).

[78] Many believe that cybersecurity is offense dominant because hackers launch millions of unattributable attacks on computers worldwide on a daily basis. However, it's not obvious that the ease of attack at this mundane level translates into strategic offensive dominance. In fact, the difficulty and ambiguity associated with infrastructure attack may actually render cybersecurity defense-dominant at the strategic level. The offensive or defensive character of a weapon does not stem from the technology itself, but depends on the doctrinal and political context of employment; Keir A. Lieber, *War and the Engineers: The Primacy of Politics Over Technology* (Ithaca, NY: Cornell University Press, 2005). For example, entrenchment seems to be an eminently defensive tactic, yet Ulysses S. Grant relied on it to facilitate his advance on Richmond.

[79] Yet another variation on the RMA theme posed as a challenge but actually quite well accommodated by it is the "robotics revolution," described in P. W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York, NY: Penguin Press, 2009) but also three decades earlier by Paul Dickson, *Electronic Battlefield.* Unmanned vehicles feature prominently in any official discussions of RMA and NCW, so it's hard to think of them as a real alternative to it. The substitution of robot for human labor in "dull, dirty, and dangerous" jobs simply continues the trend of substituting IT for manpower described above.

but also reveal the ways in which war regularly frustrates attempts to technologically master it.[80] Contingent individual choices as well as structural constraints shape the doctrines which make technologies usable.[81] Innovations provide only fleeting advantages, and only in particular strategic and cultural contexts, because countermeasures tend to emerge quickly and because competitors eagerly copy developments.[82] In the long historical view, the RMA is just another episode in a long saga of enduring security competition among actors jockeying for relative advantage under anarchy.

Some have questioned whether this particular RMA is revolutionary at all.[83] The RMA did not emerge from whole cloth in the 1990s, as discussed above, but through incremental development of American "reconnaissance strike complexes" during the Cold War. The stage for rapid Gulf War victory in 1991 was set well in advance. From this perspective, the RMA is just the latest variation on a 20th century theme of integrated combined-arms force employment: common networks enable the different branches of a military to operate at faster tempos and over greater areas.[84] A recent volume subtitled *Creation without Destruction* shows that all four services by and large did not significantly change their Cold War procurement priorities while

---

[80] See, *inter alia*, MacGregor Knox and Williamson Murray, eds., *The Dynamics of Military Revolution, 1300-2050* (Cambridge: Cambridge University Press, 2001); John A. Lynn, ed., *Tools of War: Instruments, Ideas, and Institutions of Warfare, 1445-1871* (University of Illinois Press, 1990)

[81] Alex Roland, "The Technological Fix: Weapons and the Cost of War," U.S. Army War College, Strategic Studies Institute, 1995, states that he can identify only three instances in military history where technological choices appeared to drive strategy (Greek fire, chariots, and submarines).

[82] Colin S. Gray, "Recognizing and Understanding Revolutionary Change in Warfare: The Sovereignty of Context," U.S. Army War College, Strategic Studies Institute, 2006; Benbow, *Silver Bullet?*. There is some debate over how easily the IT RMA might diffuse to other powers given the high degree of asset-specific knowledge and industrial expertise required to realize it; Emily O. Goldman and Leslie C. Eliason, eds., *The Diffusion of Military Technology and Ideas* (Stanford, CA: Stanford University Press, 2003); Barry D. Watts, *Six Decades of Guided Munitions and Battle Networks: Progress and Prospects* (Washington, DC: Center for Strategic and Budgetary Assessments, 2007)

[83] Jeremy Shapiro, "Information and War: Is it a Revolution?" in *Strategic Appraisal: the Changing Role of Information in Warfare*, ed. ZalmayKhalilzad (Santa Monica, CA: RAND, 1999): 113-153

[84] Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton, NJ: Princeton University Press, 2004) argues that militaries which employ the "modern system"—the integrated use of cover, concealment, dispersion, fire suppression, and independent maneuver by mutually-supporting infantry, artillery, armor, air, *etc.*—can better survive and thrive amidst the lethality of industrialized battlefields by blunting the effects of technological or numerical superiority alone. Biddle criticizes narrow visions of the RMA which reduce war to a long-range targeting problem because that does not employ the modern system of combined arms maneuver on the ground, thereby placing too much faith in technology alone rather than integrated force employment; Stephen Biddle, "The Past As Prologue: Assessing Theories of Future Warfare," *Security Studies* vol. 8, no. 1 (1998): 1-74. While Biddle's basic point that the management of complexity is more important than technological capabilities or numerical preponderance, the intimate relationship of technology to complexity management singles out IT as especially worthy of closer examination, vice just treating the generic role of "technology" in militaries.

fielding RMA capabilities.[85] Another study concluded that the U.S. defense industry was already organized about as well as could be hoped, given the profound political-economic distortions that exist in that field, for developing the core capabilities of the Transformation agenda such as unmanned vehicles and littoral combat ships.[86] Academic scholarship on the RMA has tended to take a jaundiced view, finding more evolutionary rather than revolutionary change in a broader historical context, and putting doctrinal debates and bureaucratic politics ahead of technology in determining change. This is all a useful corrective to the excesses of RMA enthusiasm. At the same time, it tends to obscure whatever novel opportunities and challenges might come with ubiquitous adoption of IT and growing knowledge-intensiveness in military organizations.

2.3.3 Clausewitz Don't Surf!

Many critics take Clausewitzian "fog of war" as an axiom and take the RMA camp to task for assuming that perfect knowledge is possible. Their concern is less that the enemy will attack information systems as feared by the cybersecurity camp, and more that blind spots will be generated by an organization's own reliance on IT. Overdependence on C4ISR would thus leave a resourceful enemy with space to survive, adapt, and exploit RMA forces' ignorance and failure to adapt.[87] Benbow observes that with too many moving parts, unpredictable breakdowns, human error, and enemy resistance, "far from reducing the potential for friction, the envisaged systems involve greater possibilities for it to occur."[88]

In one of the first scholarly treatments of command and control, Martin van Creveld described the "information pathologies" which plagued the American Army in Vietnam.[89] Pervasive electronic communications enabled commanders and bureaucrats to get involved in

---

[85]Harvey M. Sapolsky, Benjamin H. Friedman, and Brendan R. Green, eds., *US Military Innovation after the Cold War: Creation without Destruction* (New York, NY: Routledge, 2009). The only truly innovative change in the DoD, the authors observe, is the emergence of U.S. Special Operations Command (SOCOM) as "the fifth service," to be discussed in Chapter 7.

[86]Peter J. Dombrowski and Eugene Gholz, *Buying Military Transformation: Technological Innovation and the Defense Industry* (New York, NY: Columbia University Press, 2006).

[87]Stephen Biddle, "The Past As Prologue: Assessing Theories of Future Warfare," *Security Studies* vol. 8, no. 1 (1998): 1-74; Michael E. O'Hanlon, *Technological Change and the Future of Warfare* (Washington DC: Brookings Institution Press, 2000); Colin S. Gray, *Weapons Don't Make War: Policy, Strategy, and Military Technology* (Lawrence, KS: University Press of Kansas, 1993)

[88]Benbow, *Magic Bullet?*, 92

[89] Van Crevald, *Command in War*, 232-260. See also George S. Eckhardt, *Vietnam Studies: Command and Control 1950-1969* (Washington, DC: Department of the Army, Center of Military History, 1974)

tactical action and so they did. Circuits were overloaded and planning times drawn out, which in turn led to a proliferation of classification markings and more circuits. Workarounds to shortfalls in reporting processes, like the infamous image of helicopters stacked in the air so that each echelon commander could observe and intervene in the events on the ground below, added to the confusion of command. The rise of econometric systems analysis, a favored tool of Defense Secretary Robert McNamara, created a demand for quantitative data which kept staffs busy collecting and displaying statistics but hindered their understanding of political and military nuances on the ground. "Designed to produce accuracy and certainty, the pressure exercised from the top for more and more quantitative information ended up by producing inaccuracy and uncertainty."[90] Three decades later the U.S. invaded Afghanistan and Iraq with the most networked force in history, yet deployed forces still had to struggle through information pathologies.[91]

2.3.3.1 The Fog of War

The invasions seemed to start with the RMA playbook: highly-networked, intelligence-driven, and very Joint forces rapidly defeated quantitatively-superior conventional formations of armor and infantry. However, while these opening episodes were won handily with few casualties, they did not really conform to the RMA model. In Afghanistan in 2001 American air power and special operations needed the Afghan Northern Alliance on the ground, a motivated but rudimentary conventional army, to defeat Taliban forces in the field.[92] The U.S. furthermore failed in one of its primary objectives of capturing Osama bin Laden, who slipped through the American reconnaissance net in the Battle of Tora Bora.[93]

RMA visions of "shock and awe" in Iraq ran afoul of internal computer problems and stiff irregular resistance. The 1st Marine Division lessons-learned report observes:

> Intelligence sections at all levels were inundated with information and data that had little bearing on their mission or Intelligence requirements ... It seemed that all data, information, and products were being pushed through overburdened

---

[90] *Ibid.*, 259

[91] Milan N. Vego, "Operational Command and Control in the Information Age," *Joint Forces Quarterly* vol. 35 (2003): 100-107

[92] Stephen D. Biddle, "Allies, Airpower, and Modern Warfare: The Afghan Model in Afghanistan and Iraq," *International Security* vol. 30, no. 3 (2005): 161-176

[93] Peter J. P. Krause, "The Last Good Chance: A Reassessment of U.S. Operations at Tora Bora," *Security Studies* vol. 17, no. 4 (2008): 644 - 684

> communications paths with little thought to who needed what and when they needed it. The burden of sifting through tremendous amounts of raw data fell to each [command's] already overburdened intelligence section.[94]

This overload of irrelevant information from higher echelons then turned into a trickle once combat operations began:

> After crossing the Line of departure, the Division received very little actionable intelligence from external intelligence organizations...The nature of the battlefield, the extreme distances, high operational tempo and lack of a coherent response from a conventional enemy all made it difficult for an external agency to know what was tactically relevant and required by the [ground] commander. The byzantine collections process inhibited our ability to get timely responses to combat requirements with the exception of assets organic to or [in direct support] to the Division...*The Division found the enemy by running into them, much as forces have done since the beginning of warfare.*[95]

As the mechanized advance ran into fierce irregular resistance, engagements like the Marine assault on an-Nasiriyah were "marked by confusion, indecisiveness, and costly mistakes."[96] A multi-ship Apache helicopter attack foundered when the lights of an entire town blinked off to signal the Iraqis below to begin an ambush with small arms and antiaircraft artillery fire.[97] Higher headquarters overlooked tactical obstacles that did not appear on their Common Operational Picture, which displayed only the Iraqi Republican Guard and regular Army units that had been designated as the enemy before the war, even after the irregular Saddam Fedayeen had emerged as one of the most significant threats on the battlefield:

> [Land component commander Lieutenant General David] McKiernan made a telling comment to his staff: 'Blue Force Tracker drives the CINC [U.S. Central Command, Commander in Chief, General Tommy Franks]'...On the CENTCOM computer screens, the blue icons that represented the Army had not been moving north, and it was easy to conclude that fighting had ceased when in fact the Army had been contending with the Fedayeen. If the scale of the map was reduced to a specific area, however, the screen showed considerable activity. The blobs of

---

[94] 1st Marine Division, "Operation Iraqi Freedom (OIF): Lessons Learned," May 2003, 11.

[95] *Ibid.*, 4, emphasis added. A similar story is told in David Talbot, "We Got Nothing until They Slammed intoUs," *Technology Review*, November 2004: 107-115; victory at Objective Peach resulted came from well-trained crews and the capabilities of the M1A1 tank rather than ISR cueing.

[96] Michael R. Gordon and Bernard E. Trainor, *Cobra II: The Inside Story of the Invasion and Occupation of Iraq* (New York: Random House, 2006), 258

[97] *Ibid.*, 271-2

> blue icons on the screens—representing all of southern Iraq—at CENTCOM headquarters in Qatar or at the Pentagon had been interpreted incorrectly, McKiernan thought...The ground war had started fast and accelerated...But the speedy attack had stalled when the Fedayeen had surprisingly struck back. The top military commanders at CENTCOM and the land war command were at odds as to what to do next.[98]

In this instance, the systems that were supposed to lift the fog of war for the Modern Alexander actually blinded commanders to events unfolding on the ground. Shock and awe devolved into bloody frustration as guerrilla resistance blended in with civilian populations in order to defeat American targeting. Instead of just networks of sensors and shooters to identify and engage targets, these fights demanded boots on the ground for human intelligence gathering, negotiation with local elites, and reconstruction of civil infrastructure and society. Just as the bursting of the dotcom bubble in 2000 undermined hype for the new information economy, so the insurgencies in Afghanistan and Iraq shattered hopes for high-tech low-cost victory. The RMA had "multiplied American strengths but not reduced American weakness."[99]

2.3.3.2 Irregular War

In the 1990s some critics worried that "Faith in an RMA could reinforce the military penchant for defining missions and capabilities in terms of large-scale conventional warfare."[100] In the next decade their fears were borne out. The RMA was not the only vision of future war to emerge after the Cold War. Another prevalent view was that irregular non-state actors would wage terror and insurgency campaigns against advanced industrialized states from the sanctuary of failed states.[101] This school of thought emphasizes the importance of constabulary, special

---

[98] *Ibid.*, 314

[99] John Robert Ferris, "Netcentric Warfare, C4ISR and Information Operations: Towards a Revolution in Military Intelligence?" *Intelligence and National Security* vol. 19, no. 2 (2004): 199-225. In general, when intelligence is consistent with what commanders arealready inclined to do then it helps them to do it better, but when it is not they ignore it; see, for example, the excellent study by Edward Drea, *MacArthur's Ultra: Codebreaking and the War Against Japan: 1942-1945* (Lawrence, KS: Kansas University Press, 1992)

[100] Richard K. Betts, "The Downside of the Cutting Edge: Disadvantages of Revolution in Military Affairs," *The National Interest* (Fall 1996). Betts also notes that not only might the RMA incentivize irregular counter-RMAs, but also it might contribute to crisis instability with conventional opponents by holding their deterrent forces at risk.

[101] This literature is perhaps even broader and more uneven than that on the RMA. See, for example, Martin Van Creveld, *The Transformation of War* (New York, NY: Free Press, 1991). More recently, the failed state terrorism nexus is summed up by Defense Secretary Robert M. Gates, "Helping Others Defend Themselves," *Foreign Affairs* vol. 89, no. 3 (2010): 2-6, "In the decades to come, the most lethal threats to the United States' safety and security - a city poisoned or reduced to rubble by a terrorist attack - are likely to emanate from states that cannot

operations, and counterinsurgency operations. The actual U.S. campaigns of the 1990s—in Haiti, Somalia, Bosnia, Colombia, and Kosovo—more resembled this vision of low-intensity conflict. But as we have seen, the RMA vision was more institutionalized in the Defense Department and defense industry.[102]

After the terrorist attacks of 11 September 2001 and the ongoing wars in Central Asia, the counterinsurgency vision received more emphasis. This vast literature is beyond the scope of this chapter to assess.[103] Suffice it to say that its expectations for war are almost the opposite of the RMA vision: irregular campaigns are expensive gambles that last for years; they are confusing, highly-politicized, and prone to failure; they require large numbers of troops on the ground for institution building and face-to-face human interaction with indigenous populations; intelligence depends on human informants more than signal intercepts; force must be used sparingly because mistakes can undermine everything; marketing and persuasion or "information operations" should be the main effort.

A military optimized for network-centric warfare thus invites three tragic failures on an irregular battlefield. First, the RMA emphasizes quick, decisive, offensive action; however, this

---

adequately govern themselves or secure their own territory. Dealing with such fractured or failing states is, in many ways, the main security challenge of our time." (2)

[102] While American procurement and training priorities did not align with this "most formidable threat," the emergence of RMA counters could hardly be considered a surprise. The seminal 1992 net assessment on the RMA from Andrew Marshall's office was eerily prescient on the severity of the challenge: "the most formidable threat the United States will face over the next 10-20 years as this [RMA] develops more fully will be a Third World competitor that combines some of the sophisticated technologies of the Cold War era with the unconventional strategies [that negate the effectiveness of the RMA]...Assume also that this state is energized by an ideology hostile to our values, or by a radical theocratic leadership...the aggressor would attempt to exploit those aspects of the U.S. social culture that would inhibit the effective application of American military power. Specifically, acts of aggression would be low-intensity in nature and ambiguous in execution, with emphasis on terrorism, subversion, and insurgency" (Krepinevich, "Military-Technical Revolution," 46-47).

[103] Chapters 5 and 7 will return to counterinsurgency in more depth. The official U.S. doctrinal version, developed for the Iraq War under the leadership of General David Petraeus (and the only Army manual ever to show up on the New York Times bestseller list), is U.S. Army, *Field Manual 3-24: Counterinsurgency* (Washington DC: U.S. Government Printing Office, 2006). Notable COIN texts include, *inter alia*, David Galula, *Counterinsurgency Warfare: Theory and Practice* (London: Praeger Security International, 2006); Roger Trinquier, *Modern Warfare: A French View of Counterinsurgency* (London: Praeger Security International, 2006); Frank Kitson, *Low Intensity Operations: Subversion, Insurgency, Peace-Keeping* (Harrisburg, PA: Stackpole Books, 1971); Robert Taber, *War of the Flea: The Classic Study of Guerrilla Warfare* (Washington, DC: Potomac Books, 2002); Stephen T. Hosmer and Sibylle O. Crane, *Counterinsurgency: A Symposium, April 16-20, 1962* (Santa Monica, CA: RAND Corporation, 1962), http://www.rand.org/pubs/reports/2006/R412-1.pdf; Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (New York, NY: Penguin Books, 2006); Anthony James Joes, *Resisting Rebellion: The History and Politics of Counterinsurgency* (University Press of Kentucky, 2006).

"first mover advantage" becomes counter-productive in situations where it would be better to deliberately develop an understanding of the situation by talking to and observing the locals. Second, reliance on architectures built for targeting enemies can impede adaptation to the counterinsurgency problem by biasing operations towards offensive targeting and away from negotiation and civil affairs. Like Sisyphus, continuous tactical successes fail to deliver and may even undermine strategic objectives, while impeding exploratory learning.[104] Third, irregular adversaries, who are not locked into any infrastructure, can exploit commoditized commercial IT and the internet to enhance their communication, recruitment, training, intelligence, propaganda, as well as design novel and lethal improvised explosive devices (IEDs) to ambush troops and kill civilians. In sum, the RMA may enable militaries to react too quickly and in the wrong way, and then slow their adaptation to better ways, all the while pitting them against adversaries for whom commercial IT has provided enhanced capability. The human-centric counterinsurgency camp argues that the network-centric RMA camp predicted the wrong revolution.[105]

2.3.3.3 Service Differences

The most outspoken criticism of the RMA and some of the most poignant examples of IT failure in combat tend to come from the ground-oriented services.[106] The Army and Marine Corps have to coordinate tens or hundreds of thousands of individuals in an ambiguous environment filled with friendly, neutral, and hostile populations. Ground forces are more likely to literally come face to face with their adversaries and allies, so it is not surprising that such officers attack the RMA for underweighting moral and psychological elements. War is not just a targeting drill among edges and nodes, but a contest between willful adversaries with unpredictable and bloody consequences. "Just-in-time" logistics are liable to founder when

---

[104]Colin F. Jackson, "Defeat in Victory: Organizational Learning Dysfunction in Counterinsurgency," Ph.D. Dissertation, Massachusetts Institute of Technology, 2008. Soldiers refer to this experience variously as "Groundhog Day" after the movie in which Bill Murray's character wakes up to the same day over and over again, "Whack-a-Mole" in reference to the arcade game that involves endlessly bopping rodents with a mallet as they pop up, and "mowing the grass" which just keeps growing back.

[105]Frank G. Hoffman, "Complex Irregular Warfare: The Next Revolution in Military Affairs," *Orbis* vol. 50, no. 3 (2006): 395-411; Kagan, *Finding the Target*; James N. Mattis, "USJFCOM Commander's Guidance For Effects-Based Operations," *Joint Forces Quarterly*, no. 51 (2008): 105-108

[106] See, for example, John A. Gentry, "Doomed to Fail: America's Blind Faith in Military Technology," *Parameters* vol. 32, no. 4 (2002); H.R. McMaster, "Crack in the Foundation: Defense Transformation and the Underlying Assumption of Dominant Knowledge in Future War," US Army War College Center For Strategic Leadership, Student Issue Paper S03-03, 2003. The hostility of Army officers to the RMA is by no means absolute; for a sanguine Army perspective on the RMA, *cf.* Gordon R. Sullivan and Anthony M. Coroalles, "The Army in the Information Age," U.S. Army War College, Strategic Studies Institute, 1995.

convoys come under attack. Systems are prone to breakdown due to bad weather and accident, and design assumptions are often ill-suited to the creative responses of opponents who actively seek out the limitations of targeting systems.

By contrast the most spirited defense of the RMA tends to come from the more technology-oriented services. The Navy and Air Force are built around smaller numbers of expensive technological platforms which operate in relatively homogenous domains devoid of permanent civilian presences.[107] Networked operations are not only more possible, but also necessary for the coordination of fast-moving machines over vast stretches of sea and aerospace. Sailors and airmen are thus more likely to experience instances where IT is an invaluable force multiplier. In arguing that IT-enabled rationalization can indeed reduce the uncertainties of the past, they argue that the fog-of-war objection a reactionary canard.[108]

2.3.3.4 The Revolution is Offensive

Critics have also raised alarms over the moral consequences of remote-control warfare. Perceptions of RMA-enabled offense-dominance ("victory is easy") might tempt policy makers to foolishly launch wars with the expectation of low costs and rapid victory, only to have to pay far more in the grinding attrition which inevitably ensues after assumptions prove unrealistic. The same problem at the tactical level could create unacceptable collateral damage as illusions of certainty promote hasty targeting decisions, or as ambiguity over civilian and military targets erode considerations of proportionality. Soldiers may lose contact with the visceral experience of combat and treat war as a video game, becoming more willing to slaughter innocents and inured to the consequences. RMA forces may unintentionally send messages of vulnerability or callousness to the indigenous populations who observe and experience remote strikes, generating resentment and backlash (i.e., "Americans are too cowardly to fight us like men, so they send their robots to kill us like insects.").[109]

---

[107] Those segments of air forces and navies which work closely with ground forces, such as close air support and amphibious operations, should be expected to have more in common with the ground-based outlook.

[108] *E.g.*, Phillip S. Meilinger, "A History of Effects-Based Air Operations," *Journal of Military History* vol. 71, no. 1 (2006): 139-167; Jeffery R. Barnett, "Defeating Insurgents With Technology," *Airpower Journal*, Summer 1996

[109] Andrew J. Bacevich, "Just War II: Morality and high technology," *The National Interest*, no. 45 (Fall 1996): 37-48; David J. Betz, "The More You Know, the Less You Understand: The Problem With Information Warfare," *Journal of Strategic Studies* vol. 29, no. 3 (2006): 505-533; Robert Mandel, "The Wartime Utility of Precision Versus Brute Force in Weaponry," *Armed Forces & Society* vol. 30, no. 2 (2004): 171-201; Charles J. Dunlap, Jr., "Technology and the 21st Century Battlefield: Recomplicating Moral Life For the Statesman and the Soldier," U.S. Army War College

2.3.4 Not a Panacea, but Still Indispensible

This dissertation is sympathetic with all of these criticisms; it presents a theory of information *friction* after all. Yet the fog-of-war pessimism sometimes goes too far. The same after-action reports that complain of IT dysfunction can also be mined for anecdotes of network-enabled success stories.[110] Ground forces, although (or because) they have to contend with an ambiguous and human-focused battlefield, maintain a healthy appetite for intelligence support at all echelons, "blue force tracking" to keep track of friendly formations and avoid fratricide, "information operations" to communicate messages to populations, and databases and collaboration tools for staff coordination. The same reports from the field that note frustration with existing IT often look right back to more IT for the solutions; for example, the U.S. 3rd Infantry Division reported that "there was not enough commonality between user functions, graphical displays, and optional features, even to the level of computer operating system. The future requirement for these systems is a one-stop compatible hardware and software package to synchronize all of the [systems] within the unit."[111] To paraphrase, when computers are broken, buy better computers.

U.S. forces have actually increased their investment in sensors, networks, and remote precision strike since the latest spate of irregular wars in Central Asia began. If RMA fantasies were suited only to combat Soviet hoards in Central Europe or to replay the first Gulf War, then we might expect them to subside after a decade of ongoing combat experience of a very different sort in Afghanistan and Iraq. Instead, as discussed in the first part of this chapter, computational networks have grown more robust at all levels of command. Two orders of magnitude more unmanned vehicles have been introduced onto the battlefield, from a few hundred aerial drones to tens of thousands of robots of all types. Military personnel have access to many new

---

Strategic Studies Institute, January 1999; Thomas W. Smith, "The New Law of War: Legitimizing Hi-Tech and Infrastructural Violence," *International Studies Quarterly* vol. 46 (2002): 355-374; Seyom Brown, *The Illusion of Control: Force and Foreign Policy in the Twenty-First Century* (Washington, DC: Brookings Institution Press, 2003)

[110] The same Marine report cited above (n. 94) also includes the following item, praising a system which provided intranet connectivity and improved situational awareness: "The Trojan Spirit systems were a godsend. They provided access to the daily CFLCC briefs, NIMA products, IESS and external collections products, etc. These were all critical to the Division and RCT collections shops to keep their situational awareness and provide tactically relevant intelligence tailored to their commander's requirements. TS also allowed access to real time SIGINT reporting through AMHS, and monitor Zircon chat. The TS systems also provided an all-weather, all-distance telephone link that was used frequently to pass critical time-sensitive intelligence to RCT commanders when other communications links were unreliable or otherwise unavailable" (5).

[111] 3rd Infantry Division, After Action Report from Operation Iraqi Freedom, 2003

information systems that didn't exist in 2003. Some observers have credited the highly-networked, intelligence-intensive and targeting-oriented Special Operations Command—with its informal slogan "it takes a network to fight a network"—for contributing significantly to the drop in violence in Iraq.[112] Air Force Secretary Michael noted the "expectation of combatant commanders for situational awareness 24/7/365" from aerial surveillance: "that appetite has been established and I do not see that changing."[113]

While the U.S. military *did* build new counterinsurgency capabilities, it *also* built more RMA systems, rather than trading one for another. It turns out that computers *are* useful in irregular war, even if they sometimes get used differently (and perhaps more ominously) than in the orthodox net-centric vision. Counterinsurgency applications emphasize social control measures and Orwellian surveillance of the indigenous population.[114] Perhaps the strongest statement of complementarity comes from the U.S. Army's foremost champion of counterinsurgency doctrine and lead author of its best-selling manual on the subject, General David Petraeus. As commander of Multi-National Forces in Iraq in 2007, Petraeus expressed great enthusiasm for the RMA:

> It's definitely here to stay. It's just going to keep getting greater and greater and greater...I was a skeptic of network-centric warfare for years...[But after wartime investment we now have the ability] to transmit data, full-motion video, still photos, images, information. So you can more effectively determine who the enemy is, find them and kill or capture, and have a sense of what's going on in the area as you do it, where the friendlies are, and which platform you want to bring to bear...We realized very quickly you could do incredible stuff with this...It was revolutionary. It was.[115]

Military effectiveness is not about absolute levels of capability, but rather performance relative to adversaries. It's not necessary that IT capabilities provide perfect knowledge to

---

[112]Discussed further in Chapter 5. Bob Woodward, "Why Did Violence Plummet? It Wasn't Just the Surge," *Washington Post* (8 Sept 2008): A9

[113]Gordon Lubold, "As drones multiply in Iraq and Afghanistan, so do their uses," *Christian Science Monitor*, 2 March 2010

[114]Martin C. Libicki, David C. Gompert, David R. Frelinger and Raymond Smith, *Byting Back: Regaining Information Superiority Against 21st-Century Insurgents, RAND Counterinsurgency Study, Volume 1* (Santa Monica, CA: RAND, 2007)

[115]Noah Shachtman, "How Technology Almost Lost the War: In Iraq, the Critical Networks Are Social—Not Electronic," *Wired* (27 November 2007). That title is the best one-sentence summary of the counterinsurgency camp's criticism of the RMA.

improve military performance, but just enough situational awareness to improve competitive performance.[116] This then shifts the problem to the conditions under which IT can be expected to enable and constrain military performance, rather than an argument over its absolute effect.

To sum up, RMA debates have often been stuck in a polarized argument about IT's effects. While visionary optimism has often been too great, excessive pessimism is not warranted either. In real military organizations, information systems are never finished, control is never assured, and personnel struggle with machines and with each other to figure out how to process information, which layers on complexity and frustrates efforts to understand it all in detail. The tensions that Janowitz observed between technocratic management and the rigors of warfare also play out in the use and abuse of IT, which at the end of the day provides a modicum of control over a phenomenon—war—that is inherently out of control. IT usage is indeed changing the conduct of war, but not in the deterministic ways hoped for by RMA champions. The next chapters will describe how militaries use IT to make sense of their world, and why they sometimes fail.

[116]Barry D. Watts, "Clausewitzian Friction and Future War, Revised Ed." National Defense University, McNair Paper no. 68 (2004)

Chapter 3: Information Friction and its Effects

> "Conscious of the gigantic and infinite results to spread from that little piece of paper, all four of us felt our hearts tighten." – French Minister of War Adolphe Messimy, on delivering the order to mobilize, 1 August 1914.[1]

3.1 Defining Information Friction

While information technology (IT) usage can sometimes improve military effectiveness, it can also amplify bureaucratic pathologies. This chapter draws on interdisciplinary concepts from security studies, sociology of technology, and cognitive science to develop the notion of *information friction* to explain how the "fog of war" persists in IT-intensive militaries and why it matters for battlefield performance.

3.1.1 Drawing on the Sociology of Technology

The "revolution in military affairs" (RMA) literature reviewed in the previous chapter assumes that the information revolution causes radical changes in warfare. Historians and sociologists have mounted a sustained attack on the general notion that a technology's intrinsic nature could propel history in a certain direction.[2] Instead scholars emphasize the political and cultural contexts that shape choices to employ technologies, often with quite unintended consequences.[3] This does not mean that technology is a neutral substance; quite the contrary,

---

[1] Barbara W. Tuchman, *The Guns of August* (New York, NY: Random House, 1994), 89

[2] Merritt Roe Smith and Leo Marx, ed., *Does Technology Drive History? The Dilemma of Technological Determinism* (Cambridge, MA: MIT Press, 1994)

[3] Useful overviews and representative scholarship from this interdisciplinary field include, *inter alia*, from the history of technology: David E. Nye, *Technology Matters: Questions to Live With* (Cambridge, MA: MIT Press, 2006); Thomas P. Hughes, *Human-Built World: How to Think about Technology and Culture* (Chicago, IL: Univesity of Chicago Press, 2004). From the sociology of scientific knowledge (SSK) see Steven Shapin, "Here and Everywhere: Sociology of Scientific Knowledge," *Annual Review of Sociology* vol. 21 (1995): 289-32; Bruno Latour, *Science in Action: How to Follow Scientists and Engineers through Society* (Cambridge, MA: Harvard University Press, 1988). On the social construction of technology (SCOT) see: Wiebe Bijker, Thomas P. Hughes and Trevor Pinch, ed. *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (Cambridge, MA: MIT Press, 1987); Donald A. Mackenzie and Judy Wajcman, ed. *The Social Shaping of Technology, 2nd Ed* (Philadelphia, PA: Open University Press, 1999). From the related science, technology, and society (STS) perspective see Lucy A. Suchman, *Human-Machine Reconfigurations: Plans and Situated Actions, Revised* Edition (New York: Cambridge University Press, 2006). On the sociology of technology in corporate organizations see Wanda J. Orlikowski, "Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations," *Organization Science* vol. 11, no. 4 (2000): 404-428; Jeffrey K. Liker, Carol J. Haddad and Jennifer Karlin, "Perspectives on Technology and Work Organization," *Annual Review of Sociology* vol. 25 (1999): 575-596. There is also a vast literature on the political economy of science and technology, *e.g.*, Vernon W. Ruttan, *Technology, Growth, and Development: an Induced Innovation Perspective* (Oxford University Press, 2001)

social actors actively shape artifacts to transform or reinforce other institutional elements.[4] A speed bump, for example, is an architectural form of regulation to enforce a speed limit; Lawrence Lessig thus argues that "code is law" for internet protocols that empower one political actor at the expense of others.[5] Geoff Bowker and Leigh Star similarly observe that "software is frozen organizational and policy discourse" which gives inertia to the resolution of political controversies.[6] Technologies become politicized as people seek to control their design in order to lock-in assumptions and shape future behavior.[7] This idea echoes Terry Moe's argument that politicians create bureaucracies to lock in favored interests beyond their incumbencies, while their rivals try to hobble them by the same logic.[8]

Technology is an essential part of the fabric of modern institutions—along with laws, norms, and the means of their enforcement—and it gets caught up in the same kind of politics.[9] This holds especially for *information technology* since, as Nobel laureate Douglass North writes, "Information processing by the actors as a result of the costliness of transacting underlies the formation of institutions."[10] The growth of modern state power is everywhere accompanied by an increase in bureaucrats making, populating, and comparing lists, diagrams, and files.[11] James Scott in *Seeing Like a State* describes how:

---

[4] Langdon Winner, "Do Artifacts Have Politics?" *Daedalus* vol. 109, no. 1 (1980): 121-136; W. Richard Scott, "Institutional Carriers: Reviewing Modes of Transporting Ideas over Time and Space and Considering their Consequences," *Industrial and Corporate Change* vol. 12, no. 4 (2003): 879-894

[5] Lawrence Lessig, "The New Chicago School," *Journal of Legal Studies* vol. 27, no. 2 (1998): 661-691; Lawrence Lessig, *Code, Version 2.0* (New York, NY: Basic Books, 2006)

[6] Geoffrey C. Bowker and Susan Leigh Star, *Sorting Things Out: Classification and Its Consequences* (Cambridge, MA: MIT Press, 1999), 135.

[7] Donald A. Mackenzie, *Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance* (Cambridge, MA: MIT Press, 1993), 340-381; Wanda J. Orlikowski, "The Duality of Technology: Rethinking the Concept of Technology in Organizations," *Organization Science* vol. 3, no. 3 (1992): 398-427.

[8] Terry M. Moe, "Political Institutions: The Neglected Side of the Story," *Journal of Law, Economics, & Organization* vol. 6 (special Issue 1990): 213-253; Amy Zegart, *Flawed by Design: The Evolution of the CIA, JCS, and NSC* (Stanford, CA: Stanford University Press, 1999)

[9] W. Brian Arthur, *The Nature of Technology: What It Is and How It Evolves* (New York, NY: Free Press, 2009), comes close to actually defining economic institutions themselves as a sort of technology.

[10] Douglass C. North, *Institutions, Institutional Change, and Economic Performance* (Cambridge University Press, 1990), 107. North uses a sports metaphor to define institutions as "the rules of the game," both formal and informal as well as their enforcement by a league, which constrain the organizational "players." Technology would thus be the "equipment" and the "playing field," subject to constraint by rules but also offering up opportunities and constraints beyond those explicitly articulated (like the spitball before it was banned in baseball). North argues that "Together with the technology employed, [institutions] determine transaction and transformation costs and hence the profitability and feasibility of engaging in economic activity" (118).

[11] Michel Foucault, *The Order of Things: An Archaeology of the Human Sciences* (New York: Vintage, 1994)

> processes as disparate as the creation of permanent last names, the standardization of weights and measures, the establishment of cadastral surveys and population registers, the invention of freehold tenure, the standardization of language and legal discourse, the design of cities, and the organization of transportation seemed comprehensible as attempts at legibility and simplification. In each case, officials took exceptionally complex, illegible, and local social practices, such as land tenure customs or naming customs, and created a standard grid whereby it could be centrally recorded or monitored...The social simplifications thus introduced not only permitted a more finely tuned system of taxation and conscription but also greatly enhanced state capacity. They made possible quite discriminating interventions of every kind, such as public-health measures, political surveillance, and relief for the poor. [12]

The emergence of standard measures of time, distance, money, and number in the 12th century, combined with techniques to visualize the results, contributed to the emergence of European modernity by facilitating more efficient economic exchange and imperial conquest.[13] An information revolution of sorts in the eighteenth century—dictionaries, maps, and classification schemes—laid in groundwork for the industrial revolution by popularizing notions of standardization and rationalization.[14] As sprawling industries arose around the turn of that century, filing cabinets, standardized forms, copying and tabulating machinery, and other novel information management techniques facilitated more efficient corporate management.[15] Global telegraph and telephony provided imperial metropoles with control over far flung colonies and military forces, and in the process new imperatives for communications secrecy remade

---

[12] James C. Scott, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed* (New Haven, CT: Yale University Press, 1998), 2-3

[13] Alfred W. Crosby, *The Measure of Reality: Quantification in Western Europe, 1250-1600* (Cambridge University Press, 1997); Scott, *Seeing Like a State*; North, *Institutions*.

[14] Daniel R. Headrick, *When Information Came of Age: Technologies of Knowledge in the Age of Reason and Revolution, 1700-1850* (New York, NY: Oxford University Press, 2002). For example, the management of early American railroads depended on spreadsheet-accounting techniques imported by Army officers trained in the French tradition of pedagogy at West Point, where they were used to categorize and evaluate cadets; see Keith W. Hoskin and Richard H. Macve, "The Genesis of Accountability: The West Point Connections," *Accounting, Organizations and Society* vol. 13, no. 1 (1988): 37-73.

[15] Joanne Yates, *Control Through Communication: The Rise of System in American Management* (Baltimore, MD: Johns Hopkins University Press, 1993); James W. Cortada, *Information Technology As Business History: Issues in the History and Management of Computers* (Greenwood Press, 1996); Joanne Yates, *Structuring the Information Age: Life Insurance and Technology in the Twentieth Century* (Baltimore, MD: Johns Hopkins University Press, 2005)

diplomacy and security institutions.[16] Human and IT performances are deeply intertwined in the realization of institutional processes and structures.[17]

At the same time, it is possible to take the "social construction of technology" too far towards extreme relativism. Some organizations figure out ways to use IT more productively than others, even though there appears to be a long lag time in doing so.[18] Moreover, the peculiar military job of physically destroying like kinds introduces a sobering degree of realism. Their technologies produce lethal effects, and personnel run up against hard constraints, so they want to understand just what those contraints are. To evaluate policy and to explain military performance, we need to understand not just *that* a sociotechnical system is complex with many open trajectories, but causally *how* it is complex, with what implications for effectiveness, under what conditions. We would like be able to predict when information systems are likely to break down and how we can lower the chances of that happening.

3.1.2 An Aggregate Measure of Information-Processing Problems

Information systems include all the people, machines, and data-management processes that link organizational perception and action. Any IT-intensive organization must cope with some degree of political and technical struggle to coordinate its informational structures and protocols with the world of operational concern. *Information friction* is an aggregate measure of

---

[16] Daniel R. Headrick, *The Invisible Weapon: Telecommunications and International Politics, 1851-1945* (Oxford University Press, 1991); David Paull Nickles, *Under the Wire: How the Telegraph Changed Diplomacy* (Harvard University Press, 2003); Peter J. Hugill, *Global Communications Since 1844: Geopolitics and Technology* (Baltimore, MD: Johns Hopkins University Press, 1999)

[17] Wanda J. Orlikowski and C. Suzanne Iacono, "The Truth is Not Out There: an Enacted View of the 'Digital Economy'" in *Understanding the Digital Economy: Data, Tools, and Research*, ed. Erik Brynjolfsson and Brian Kahin (Cambridge, MA: MIT Press, 2000), 352-80; Lucy A. Suchman, *Human-Machine Reconfigurations*

[18] The "productivity paradox" debate in the economic literature (so-called after Robert Solow's 1987 quip that computers appeared everywhere except in the productivity statistics) appears to have been resolved in favor of enhanced productivity. See Paul Attewell, "Information Technology and the Productivity Paradox," in *Organizational Linkages: Understanding the Productivity Paradox*, ed. D. Harris (Washington, DC: National Academy Press, 1994): 13-53; Paul A. David, "The Dynamo and the Computer: An Historical Perspective on the Modern Productivity Paradox," *American Economic Review* vol. 80, no. 2 (1990): 355-361; Thomas K. Landauer, *The Trouble With Computers: Usefulness, Usability, and Productivity* (Cambridge, MA: MIT Press, 1996). Subsequent research highlights how IT does not improve economic production all by itself; complementary organizational adaptations have been needed to exploit and shape its potential. See Erik Brynjolfsson and Lorin M. Hitt, "Beyond Computation: Information Technology, Organizational Transformation and Business Performance," *Journal of Economic Perspectives* vol. 14, no. 4 (2000): 23-48; Dale W. Jorgenson, Kevin J. Stiroh, Robert J. Gordon and Daniel E. Sichel, "Raising the Speed Limit: U.S. Economic Growth in the Information Age," Brookings Papers on Economic Activity vol. 2000, no. 1 (2000): 125-235; Bill Lehr and Frank Lichtenberg, "Information Technology and Its Impact on Productivity: Firm-Level Evidence From Government and Private Data Sources, 1977-1993," *Canadian Journal of Economics* vol. 32, no. 2 (1999): 335-362

factors which cause information systems "in the wild" to diverge from technocratic ideals of RMA performance. This theoretical notion is useful for explaining the performance and pathologies of complex control systems.[19]

Intuitively, as discussed in Chapter 1, information friction is the persistence of Clausewitzian friction on an IT-intensive battlefield. "Everything in war is simple," Clausewitz explains, "but the simplest thing is difficult. The difficulties accumulate and end by producing a kind of friction that is inconceivable unless one has experienced war....Countless minor incidents—the kind you can never really foresee—combine to lower the general level of performance so that one always falls short of the intended goal."[20] Likewise, studies of scientific laboratories show that ongoing tussles among competitors, patrons, and the equipment itself—Andrew Pickering's "mangle of practice"— take up most of scientists' time.[21] Heroic narratives of great inventors and rational progress through the scientific method leave out the frustrating material and political challenges and contingent accidents of actual discovery. So too military officers contend with "endless minor obstacles" rather than "great, momentous questions" as they struggle with IT and one another, not to mention the enemy.[22]

Many factors affect battlefield performance, ranging from the quality of weapons to the training of troops and civil-military relations. A military organization's information system is an essential intermediary for them all. It translates them into actual battlefield effects by enabling an organization to *perceive* information about the environment, *integrate* it with information in memory, and *articulate* all those material and organizational resources into battlefield behavior. Information friction, therefore, acts as a drag on everything else which affects performance.

---

[19] Kenneth N Waltz, *Theory of International Politics* (Boston, MA: McGraw-Hill, 1979), 5-6, defines a "theoretical notion" as an abstract concept, like point mass or international anarchy, that is itself neither true nor false but useful in constructing explanatory theory.

[20] Carl von Clausewitz, *On War*, trans. and ed. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 119

[21] Andrew Pickering, *The Mangle of Practice: Time, Agency, and Science* (Chicago, IL: University of Chicago Press, 1995); Shapin, "Here and Everywhere: Sociology of Scientific Knowledge"

[22] Carl von Clausewitz, *On War*, trans. and ed. Michael Howard and Peter Paret. Princeton (NJ: Princeton University Press, 1976), 120

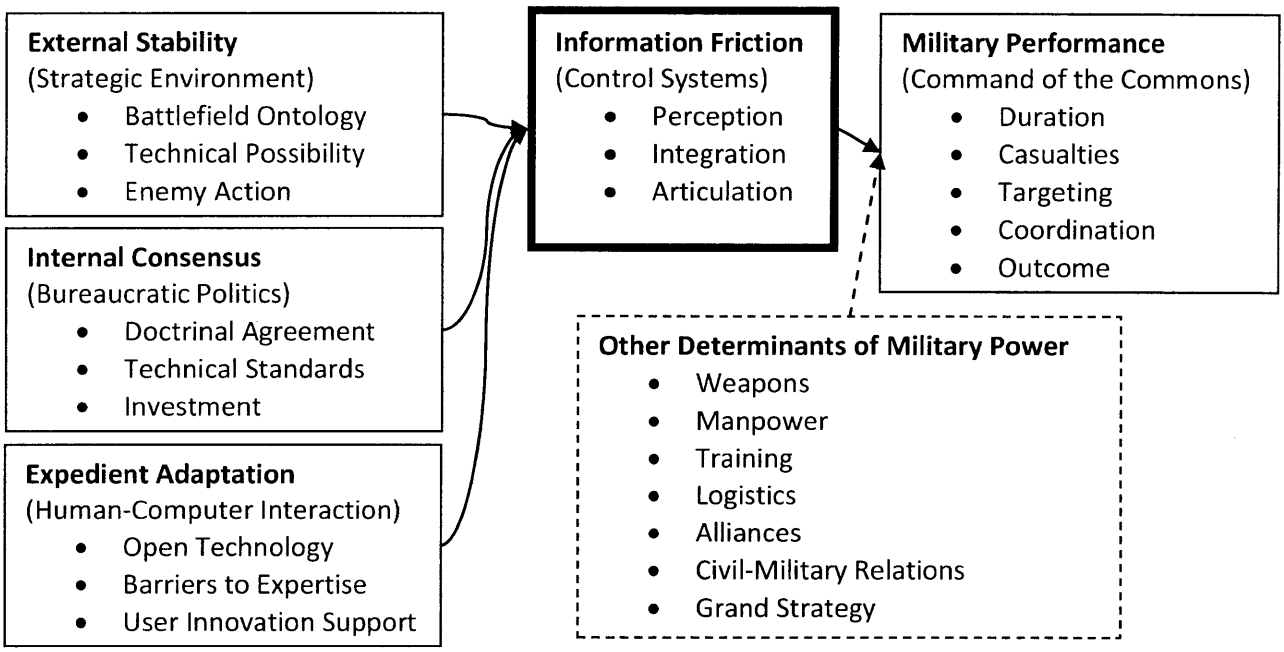


Figure 3-1: The causes and consequences of information friction

Figure 3-1 summarizes information friction theory. This chapter addresses the right side of Figure 3-1 by defining information friction and its effects. I first explain how it varies from low to high as practitioners interact with IT. I then trace the manifestations of friction in organizational control processes. I conclude with hypotheses on how information friction inversely affects military performance (*i.e.*, high friction causes low performance). I will postpone discussion of the causes of friction on the left side of Figure 3-1 until the next chapter. For explanatory convenience, this chapter examines information friction as an independent variable, and the next one takes it as a dependent variable.

3.2 Varieties of Human-Computer Interaction

Sometimes friction paralyzes an organization, but sometimes it recedes into the background. This section lays out the qualitative experience or phenomenology of two ideal types of interaction with IT.[23] Actual experience is a shifting admixture, of course.

[23] Phenomenology is systematic "first person" analysis of the structure of conscious experience, as distinguished from "third person" neurobiological accounts; see Robert Sokolowski, *Introduction to Phenomenology* (Cambridge University Press, 1999).

3.2.1 Use and Breakdown

Most computer users never think about how their operating system actually works or what a network router is doing when they send an email. At the same time, every user has experienced the frustrating inability to get important work done because of software crashes and incompatibilities. Just as bespectacled readers rarely notice the rims of their glasses while concentrating on the text, computer users usually don't pay attention to how their digital prosthetics work. When they experience a breakdown or deliberately turn their attention to technical characteristics, however, then technology emerges from the background. Likewise, the reader can consciously shift attention to the reading glasses, their optical quality, and any flecks on the lenses, while the argument of the text then recedes into the background.

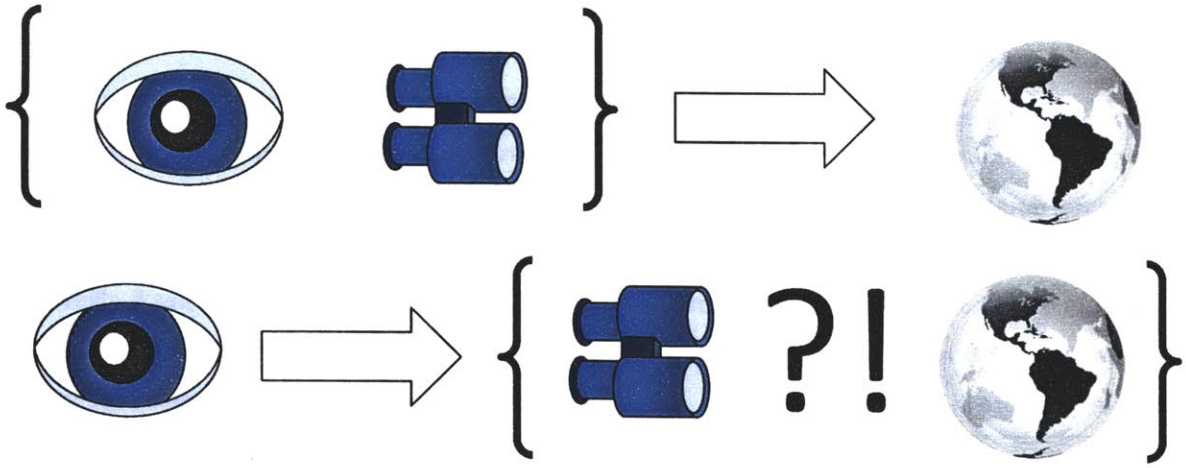


Figure 3-2: Perceptual prosthetics can be transparent or obtrusive

Figure 3-2 illustrates two *ideal* attitudes actors can take toward the IT that stands between themselves and their experience of the world.[24] Certainly people use some tools at the same time they bracket others—for example, a programmer uses an operating system while designing code that will run on it—but these are two different attitudes. In the first, technology focuses the actor's attention on substantive problems about allies, enemies, and projects in the world; the actor is like a blind man who experiences the world at the tip of his cane rather than with his hand, which is transparently taken for granted.[25] In the second, some sort of breakdown shifts

[24] Figure 3-2 adapted from Don Ihde, *Technology and the Lifeworld: From Garden to Earth* (Bloomington, IN: Indiana University Press, 1990), 86-87.

[25] Maurice Merleau-Ponty, *Phenomenology of Perception* (New York: Routledge, 2002), 261. Jean-Paul Sartre, *Being and Nothingness* (New York: Philosophical Library, 1956), similarly, describes tools as pragmatically situated

the actor's attention to the problematic relationship between means and ends; the actor turns away from concern with projects in the world toward a meta-concern with information infrastructure in bureaucratic context. Equipment failures might force such a shift, or technical design effort and scientific investigation might deliberately take up this meta-concern.[26]

3.2.2 Format and Content

The meta-concern in information systems is the relationship between *format* and *content*. I use these terms broadly to distinguish "how information works" from "what information means." The former ranges from hardware characteristics to complex social structure, and the latter from simple perception to more sophisticated acts. This is not a simple distinction between human and machine since both appear on either side of Table 3-1.

Table 3-1: Information Format and Content

Format: How information works	Content: What information means
• Computer hardware & network performance	• Perceiving signals, identities, incentives
• Software, database design, file format	• Representing & monitoring the world
• Human cognition, education, moxie	• Figuring out goals, norms, concepts, constraints
• Network & organizational policy & norms	• Understanding & judging enemies & allies
• Economic costs & regulation	• Assessing progress & prospects
• Stable structure in the environment	• Communicating, entertaining, persuading

Actors structure information format in order to maintain complex systems of reference to meaningful content. Gregory Bateson defines information as "a difference which makes a

---

in "hodological space; it is furrowed with paths and highways; it is instrumental and it is the *location* of tools" (298).

[26] Martin Heidegger, *Being and Time* (San Francisco, CA: Harper & Row, 1962), 96-102, describes this distinction with an example of hammering in a workshop. When we are caught up in the flow of making something that we care about, then the hammer is "ready-to-hand" for action in some pragmatic context. If it suddenly breaks, then the tool becomes just a "present-to-hand" object made of wood and metal. While the objective characteristics of the hammer and the workshop are "always already" there once discovered, this discovery can only happen in the context of some concern with making something and making a living. Heidegger describes the lived system of deeply-embedded and embodied references as "being-in-the-world," and other philosophers use the term "life world" for the same basic concept. The critical thrust of Heidegger's phenomenology, anticipating Thomas Kuhn's ideas on scientific paradigms, is that the objective scientific attitude is embedded in a world of concern, or an interested political project, which depends on far more "ready-to-hand" assumptions and relationships than can ever be totally unpacked and held "present-to-hand." Consciousness is an iceberg that always has more below the surface. See Hubert L. Dreyfus, *Being-in-the-World: A Commentary on Heidegger's Being and Time, Division I* (Cambridge, MA: MIT Press, 1991).

difference."[27] His first "difference" is some mark, gradient, or other physical characteristic which can be discriminated from out of the background.[28] The second "difference" is the meaning of that signal for action at some other time and place. For example, there is the invitation and the party one hopes to attend, or the target folder and the fugitive one wants to capture. The physical properties of any bits of data are never meaningful in and of themselves, but only *for* some subject *about* some object.[29] In the image of Figure 3-2 above, *format* is the binoculars and *content* is the world. IT is thus a fundamentally relational technology.

These references can break down. Under low information friction sociotechnical format recedes into the background so practitioners can focus on content. When it is high, the format is obtrusive and problematic, rendering content unavailable or unreliable. Format and content are deeply intertwined because complex information systems make sophisticated knowledge and behavior possible.

3.2.3 Uncertainty about Format and Content

The potential for breakdowns in relations of content and format highlights two different types of uncertainty.[30] "Aleatory" or stochastic uncertainty regards content and the values of known variables. Where are the enemy and friendly forces? How strong are they? What types of weapons does the enemy have? "Epistemic" or model uncertainty is about the definition of variables and methods of measurement. What kind of war am I fighting? What are my measures of effectiveness? Who needs to know?

---

[27] Gregory Bateson, *Steps to an Ecology of Mind* (Chicago, IL: University of Chicago Press, 2000), 315

[28] Mathematical information theory concerns only the transmission and discrimination of formal signals—Bateson's first difference—and thus Warren Weaver emphasizes: "The word *information*...must not be confused with meaning." Claude E. Shannon and Warren Weaver, *The Mathematical Theory of Communication* (Urbana: University of Illinois Press, 1949), 99

[29] In the philosophy of mind, "intentionality" is the capacity of something to refer to something else. Logician Franz Brentano calls intentionality "the mark of the mental," by which he means that all mental activities like seeing, knowing, judging, or appreciating all require some referential object: a subject necessarily sees, knows, judges, or appreciates *something*. Information is an inherently intentional concept. Various distinctions between syntax and semantics, medium and message, or format and content are all getting at this basic duality of information and the complications therein. Technology is not part of the brain, obviously, but if intentionality is the mark of the mental and if information is intentional, then information technology has something to do with the mind; this provides much grist for contemporary philosophy of cognitive science and artificial intelligence.

[30] J. C. Helton and W. L. Oberkampf, "Alternative Representations of Epistemic Uncertainty," *Reliability Engineering & System Safety* vol. 85 (1-3 2004): 1-10

The classic "fog of war" emphasizes aleatory uncertainty about what is happening on the battlefield. Clausewitz certainly worries about the design of military operations, especially that commanders might mistake "the kind of war on which they are embarking" or misapply bureaucratic routines "more appropriate to tactics than to strategy."[31] However, he states that "strategy uses maps without worrying about trigonometric surveys" and "even entrenchments...are not part of the conduct of war so far as *their actual construction* is concerned."[32] Today it is still conventional to assume that technical design is a peacetime affair, albeit afflicted by tremendous strategic uncertainty, which is separate from the wartime employment of weapon systems.[33]

This distinction between peacetime design of IT and wartime use is problematic. Chapter 2 described how all of the functions of command that Clausewitz worries about in the conduct of war—perceiving and understanding the battlefield, planning and executing operations, communicating with other officers, controlling the movement of troops—are now distributed across complex C4ISR networks.[34] As a result, the architecture of software and bureaucratic circuits become active operational problems. They are also sources of epistemic uncertainty. Claudio Ciborra points out that through IT, "Risk representations become more calculable and formalized, but this is obtained at the price of an incalculability of the risks of the infrastructure itself."[35] The modern "fog of war" therefore encompasses problematic IT architecture as well as whatever equivocal data appear onscreen, or epistemic uncertainty about format as well as aleatory uncertainty about content.

---

[31] Clausewitz, *On War*, 88, 153

[32] *Ibid.*, 144, 130-131 (emphasis in original); similarly, "the conduct of war has nothing to do with making guns," 144. Peter Paret, "Clausewitz," in *Makers of Modern Strategy: From Machiavelli to the Nuclear Age* (Princeton, NJ: Princeton University Press), 208, observes that "*On War* contains a comprehensive analysis of the strategy, operations, and tactics of Napoleonic war, and of their eighteenth-century background. Left out of account are most technological, administrative, and organizational factors."

[33] Rosen, *Winning the Next War*, 183-250, provides a nice discussion of the strategic sources of uncertainty over new military technology, but only discusses design uncertainty in peacetime.

[34] In fact, by Clausewitz's own criteria, IT emphatically *is* part of the conduct of war. He writes (*On War*, 152), "To the extent that *regulations* and *methods* have been drilled into troops as active principles, theoretical preparations for war are part of its actual conduct." Software is fundamentally a matter of rules, protocols, routines, methods and procedures; therefore, gyro-stabilized gun platforms, night-vision optics, database replication of intelligence data, and chatrooms that supervise unmanned surveillance flights are all built upon "active principles" coded in silicon and slavishly obedient to their drill sergeant, the software engineer.

[35] Claudio Ciborra, "Imbrication of Representations: Risk and Digital Technologies," *Journal of Management Studies* vol. 43, no. 6 (2006): 1339–1356

Table 3-2 sums up the phenomenological variance of information friction. When information friction is low, practitioners can make sense of the operational world of concern.[36] Transparent format makes content felicitously available. Participants take the harmony of political interests for granted and work toward some collective goal. They still have to deal with uncertainty, but it tends to be about the values of factors they already understand with respect to goals about which they already agree. Because their communication networks operate reliably, they can share data in order to reduce this uncertainty, which enhances their "situational awareness" and practical mastery of their circumstances, much as RMA doctrine would hope. When information friction is high, by contrast, practitioners must attend to breakdowns. Format becomes an obtrusive problem that renders content unreliable or unavailable. Breakdowns in the relationship between format and content include not just equipment faults amenable to technocratic repair, but also the politicization of representation. Participants experience intense disputes over and barriers separating informational ends and means. Technical obstacles and bureaucratic quarrels over models and methods get in the way of the mission, which itself becomes a matter of controversy.

Table 3-2: Phenomenological indicators of information friction

	Low Information Friction	High Information Friction
• Sense-making	"Situational awareness"	"Fog of war"
• Attention	{actor ⇾ tools} → world	actor → {tools ⇾ world}
• Format	Transparent usage	Obtrusive breakdown
• Content	Felicitous/available	Unreliable/unavailable
• Uncertainty	"Aleatory" values on variables	"Epistemic" models & methods
• Politicization	Harmony	Controversy

3.3 Breakdowns in Distributed Cognition

I have described information friction as the problem of breakdowns and thus uncertainties in the relationship between format and content. The rest of this chapter will take up more specific issues of *how* this relationship breaks down. It can break down in the ways people use tools to make sense of the world, and it can break down in different phases of a control process. I will begin with the cognitive functions of IT, which are the ways in which tools enable people to perform computations beyond the scope of any one individual mind. I then trace control

[36] On sensemaking in organizations in general see Karl E. Weick, *The Social Psychology of Organizing* (Reading, MA: Addison-Wesley Pub, 1979)

through the organizational *perception* of new information, *integration* with information in memory, and *articulation* of information to cause operational behavior.[37] Edwin Hutchins calls this symbiosis of humans and machines *distributed cognition.*[38] Hutchins develops the concept in a superb study of navigational practices of sailors and their instruments aboard a U.S. Navy ship, and I use it to describe military command and control in general.

3.3.1 Cognitive Prosthetics

An emerging body of work in cognitive science argues that the human mind is not a solipsistic ego inside the skull, but rather requires environmental scaffolding in a very fundamental way.[39] There are four ways in which tools which extend human mental capacities.

3.3.1.1 Affordance

All tools have *affordances*, which are features that suggest certain interactions.[40] Chairs afford sitting and cup handles afford holding-in-order-to-drink. Some design experts try to

---

[37] This terminology is from David A. Mindell, *Between Human and Machine: Feedback, Control, and Computing Before Cybernetics* (Baltimore, MD: Johns Hopkins University Press, 2002), 22-23

[38] Edwin Hutchins, *Cognition in the Wild* (Cambridge, MA: MIT Press, 1995); Edwin Hutchins, "How a Cockpit Remembers its Speeds," *Cognitive Science* vol. 19, no. 3 (1995): 265-288; James Hollan, Edwin Hutchins and David Kirsh, "Distributed Cognition: Toward a New Foundation For Human-Computer Interaction Research," *ACM Transactions on Computer-Human Interaction* vol. 7, no. 2 (2000): 174-196; Morana Alac and Edwin Hutchins, "I See What You are Saying: Action as Cognition in fMRI Brain Mapping Practice," *Journal of Cognition and Culture* vol. 4, no. 3 (2004): 629-661. The same basic phenomenon has also been variously described as *extended cognition* (Clark and Chalmers, n. 39), *epistemological engineering* (Sterelny, note 44), *collective mind* (Weick and Roberts, n. 63), and *embodied mind* (Varela *et al.*, n. 39). Computer scientists associated with the emergence of the internet also anticipate the notion of distributed cognition: J. C. R. Licklider, "Man-Computer Symbiosis," *IRE Transactions on Human Factors in Electronics* vol. 1 (March 1960): 4-11; Doug C. Engelbart, "Augmenting Human Intellect: A Conceptual Framework," Stanford Research Institute, AFOSR-3233 (1962).

[39] For the philosophical arguments that the human mind extends beyond the brain see, *inter alia*, Andy Clark and David Chalmers, "The Extended Mind," *Cognitive Science* vol. 58, no. 1 (1998): 7-19; Kim Sterelny, " Externalism, Epistemic Artefacts and the Extended Mind," in *The Externalist Challenge: New Studies on Cognition and Intentionality*, ed. Richard Schantz (New York, NY: De Gruyter, 2004): 239-254; Andy Clark, *Supersizing the Mind: Embodiment, Action, and Cognitive Extension* (Oxford University Press, 2008); Itiel E. Dror and Stevan Harnad, ed., *Cognition Distributed: How Cognitive Technology Extends Our Minds* (Amsterdam: John Benjamins Publishing Co, 2008). For more radical arguments that not only cognition (information processing) but also conscious experience depends fundamentally on embodied interaction with the environment, see: Alva Noë, *Out of Our Heads: Why You Are Not Your Brain, and Other Lessons from the Biology of Consciousness* (New York: Farrar, Straus, and Giroux, 2009); Alva Noë, *Action in Perception* (Cambridge, MA: MIT Press, 2004); Francisco J. Varela, Evan Thompson and Eleanor Rosch, *The Embodied Mind: Cognitive Science and Human Experience* (Cambridge, MA: MIT Press, 1991); Heidegger, *Being and Time*, 89: "The perceiving of what is known is not a process of returning with one's booty to the 'cabinet' of consciousness after one has gone out and grasped it; even in perceiving, retaining, and preserving, the [being] which knows remains outside."

[40] James J. Gibson, "The Theory of Affordances," in *Perceiving, Acting, and Knowing: Toward an Ecological Philosophy*, ed. Robert Shaw and John Bransford (Hillsdale, NJ: Lawrence Erlbaum Association, 1977): 67-82.

intentionally create affordances in products in order to structure and simplify the user interface.[41] However, products can also have unintentional affordances for different users. Stairs invite climbing for able-bodied people but create barriers for the disabled. A rock climber sees handholds and nooks for mechanical protection where a tourist sees only an impenetrable precipice. An affordance is a relational property between the tool and the skilled, embodied user.[42] Some sort of know-how is encoded in users' brains and bodies, but in the absence of the tool, that know-how is meaningless or inaccessible. Other information for using a tool is encoded in the very structure and logic of the tool. As roboticist Rodney Books puts it, sometimes the real world is its own best model.[43] Tools afford some actions to some users, but they can also mask actions and features.

3.3.1.2 Offload to Perception

Tools can transform difficult cognitive problems into easier perceptual ones. A bartender places paper receipts in front of each patron in order to remember their running tabs and see at a glance that they haven't yet paid. When we arrange symbols in the environment that we can physically inspect, we don't have to dedicate as much effort to remembering data and mentally computing relations.[44] We also thereby *see* concepts we wouldn't otherwise be able to think about.[45] Many people use the *PowerPoint* "slide sorter" to rearrange slides for a talk or to combine slides from multiple presentations in order to *see* what slide order makes the most sense. Some military officers use "stoplight charts" to code a large number of variables red, yellow, or green—representing material readiness, logistics status, intelligence indicators, or

---

[41] Donald A. Norman, *The Design of Everyday Things* (New York, NY: Basic Books, 1988); Donald A. Norman, "Affordance, Conventions, and Design," *Interactions, ACM* (May/June 1999); Terry Winograd and Fernando Flores, *Understanding Computers and Cognition: A New Foundation for Design* (Reading, MA: Addison-Wesley Publishing Company, Inc, 1986)

[42] Ian Hutchby, "Technologies, Texts and Affordances," *Sociology* vol. 35, no. 2 (2001): 441-456; Stuart E. Dreyfus and Hubert L. Dreyfus, "A Five-Stage Model of the Mental Activities Involved in Directed Skill Acquisition," University of California Operations Research Center, February 1980

[43] Rodney A. Brooks, *Cambrian Intelligence: The Early History of the New AI* (Cambridge, MA: MIT Press, 1999)

[44] The biology of mammalian perception is evolutionarily more ancient than higher primate cognition, so cognition builds upon ("re-purposes" or "exapts") the already-existing perceptual architecture in the brain to perform more complex computations. Kim Sterelny, *Thought in a Hostile World: The Evolution of Human Cognition* (Malden, MA: Blackwell, 2003). See also Michael Tomasello, *The Cultural Origins of Human Cognition* (Cambridge, MA: Harvard University Press, 2000); F. John Odling-Smee, Kevin N. Laland and Marcus W. Feldman, *Niche Construction: The Neglected Process in Evolution* (Princeton, NJ: Princeton University Press, 2003); Robert Boyd and Peter J. Richerson, *The Origin and Evolution of Cultures* (Oxford University Press, 2005)

[45] On the difference between action taken to achieve goals and action to arrange symbolic tokens to aid thinking about how to achieve goals, see David Kirsh and Paul Maglio, "On Distinguishing Epistemic From Pragmatic Action," *Cognitive Science* vol. 18, no. 4 (1994): 513-549; Hutchins, "How a Cockpit Remembers Its Speeds"

measures of effectiveness—in order to see what they've already analyzed and to draw attention to the most pressing problem areas. These advantages of perceptual simplification of cognition also are potential liabilities; when people just look at what is in front of them they might not think through what it means. Is a neighborhood colored green because there are no insurgents there to attack it or because insurgents control it and have no reason to attack?

3.3.1.3 Precomputation

Tools can distribute cognitive work over time and over people with different abilities. Representational structure can be "precomputed" or built up gradually in order to simplify realtime performance.[46] The update of a personal appointment calendar and automated email reminders structures one's later action in space and time. Cartographers create terrain maps by drawing on a lot of different surveying and mapmaking equipment and expertise, but map users don't have to understand or redo all that work in order to orienteer. Users can also further mark up their maps to plan their own trips so that they don't have to reconsider all the options about where to hike and where to camp. Likewise, military staffs create map overlays with battlefield control measures like the "forward edge of the battle area," "areas of operation," and "phase lines" to coordinate maneuvers and to ensure that fire plans minimize the risk of fratricide. Unfortunately, errors in precomputation might not be detected at runtime, as when a GPS system directed a man to drive into a reservoir to his death at night along a road that was no longer usable.[47] When Nicaragua dredged a portion of the San Juan River that Google's online maps marked incorrectly as its own territory, Costa Rica responded by sending 70 police officers to meet 50 Nicaraguan soldiers in escalation over the disputed border.[48]

3.3.1.4 Precision and Complexity

People use IT to manage far more relationships between things and with greater precision than any one individual would be able to manage alone. Scientific instruments in particular amplify features of the world that would be otherwise invisible, embodying measurements in the

---

[46] Hutchins, *Cognition in the Wild,* 165-169; Lucy A. Suchman, "Representing Practice in Cognitive Science" in *Representation in Scientific Practice*, ed. Michael Lynch and Steve Woolgar (Cambridge: MIT Press, 1990): 301-322

[47] Giles Tremlett, "GPS directs driver to death in Spain's largest reservoir," *Guardian* (4 October 2010)

[48] Marianela Jimenez, "OAS Urges Talks in Central America Google Map Spat," *Washington Post* (November 9 2010). A Google official gave the sardonic disclaimer that, "Although Google maps are of high quality and Google works constantly to improve and update existing information, in no way can they be used for the military decisions between two countries...It's unthinkable to rely on a product directed at consumers and business to make military decisions." Unthinkable, that is, unless thought depends on cognitive prosthetics.

physical orientation of their dials and lights on their displays which can then be translated to numbers on paper. Instruments embody theoretical and practical knowledge not captured in manuals and textbooks.[49] Thus innovations in measurement and representation often precede the articulation of new scientific theories.[50] Unfortunately the ability to track relationships of more complexity and precision than one can think about alone means that in order to interact with those things, the user becomes totally dependent on IT that is too complex to understand.

3.3.1.5 Technology and Psychology

Taking all four of these cognitive prosthetic functions together, the entire human-computer system may do things that seem rather sophisticated, but the operations that humans do by themselves are usually quite simple. Hutchins points out, "Indeed, the cognitive abilities that...practitioners employ in their use of the forms and inscriptions are very mundane ones—abilities that are found in a thousand other task settings."[51] Mundane information processing can be coupled to exotic behavior by virtue of the way IT structures the symbolic milieu. The technological infrastructure of cognition, above and beyond the psychology of individual actors, is thus a major repository of the models and assumptions that canalize organizational behavior.[52] Table 3-3 summarizes the ways in which cognitive prosthetics lower or raise information friction by either enhancing perception or risks of misperception.

Table 3-3: Information friction in cognitive prosthetics

	Low Information Friction	High Information Friction
• Affordance	Suggest appropriate action	Mask possible action
• Perceptual Offload	Reduce cognitive load	Promote uncritical acceptance
• Precomputation	Spread load over time & people	Hide assumptions
• Precision & Complexity	Sophisticated measurements	Dependency & opacity

[49] Davis Baird, *Thing Knowledge: A Philosophy of Scientific Instruments* (Berkeley, CA: University of California Press, 2004)

[50] Peter Louis Galison, *Image and Logic: A Material Culture of Microphysics* (Chicago: University of Chicago Press, 1997)

[51] Hutchins, *Cognition in the Wild*, 133

[52] Scholars and practitioners interested in misperception have usually only discussed psychological factors rather than representational tools explicitly; see Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976); Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, DC: Center For the Study of Intelligence, 1999). It is beyond my scope to tease apart psychological and technological causes of bias, which is a complicated question if the mind is indeed extended out to its environmental scaffolding.

3.3.2 Controlling Humans and Machines

Militaries use IT as a cognitive prosthesis as they address two different and difficult control problems. Armed organizations must bind fighters and flows of material into a collective goal-directed effort in a resistant environment. The adversary tries to disrupt this cooperative effort, while at the same time trying to solve its own collective action problems in order to create that disruption. The lethal symmetry between combatants—each striving to physically destroy the other—requires that both sides control themselves in order to exert control on the other. To control the enemy or to control ground, a military must be able to control itself.

Through the course of the information revolution, military self-control or C4ISR has become incredibly complex. IT provides the glue which binds together large numbers and different types of security organizations, weapons, and management tasks. Unfortunately, IT sometimes binds it all too tightly. Information friction emphasizes the difficulties that emerge in the internal control problem, which then create problems in the external control problem of defeating the enemy.

3.3.2.1 Computational Ends and Representational Means

In order to gain any sort of control, an organization must define its computational problems and implement solutions. Hutchins defines computation broadly as "the propagation of representational state across representational media," encompassing events that are internal and external to human beings.[53] The computational problem—the goal of the information system—is analytically distinct from the representational means to solve it.

Hutchins describes the difference between computational ends and representational means in two different implementations of nautical pilotage. The navigator's computational problem is to find his own location, course and speed on a two-dimensional surface by combining multiple one-dimensional constraints such as ranges and bearings to fixed landmarks and the relationship between rate, time and distance. The representational problem, by contrast, can be implemented in radically different ways. Traditional Micronesian navigators conceive of their canoe as fixed at the center of a sidereal compass with real and imaginary island reference points moving across it; they draw on nuanced oral traditions, considerable individual experience, perceptual acuity, and virtually no equipment. Western navigators, by contrast,

---

[53] *Ibid.*, 118

conceive of the chart as a fixed frame of reference with the ship moving across it; they draw on an organized division of labor, bureaucratic procedure, cartographic institutions, and specialized navigational equipment. While these two traditions actually solve the same basic computational problem by combining one-dimensional constraints on their two-dimensional location within the real world, they use radically different representational tools and processes to do so. Similar ends, different means. [54]

The definition of computational goals is not simply given, but something that an organization has to figure out, sometimes with some controversy over ends and means. When information friction is low, there is little disagreement about the computational problem and an organization's representations implements it efficiently. When it is high, there is confusion or dispute over the computational problem and collective thought is muddled by unreliable representations. The definition of computational ends and the linkage to representational means are thus political problems as much as technical ones. Institutional consensus (or disensus) over doctrinal goals in a military organization is one of the principal causes of information friction, discussed in more depth in the next chapter.

3.3.2.2 Control Cycles

Humans and machines implement representational solutions to computational problems via *control cycles*. The control cycle is a basic concept from cybernetics, a major intellectual forebear of computer engineering and cognitive science, and it applies to bureaucratic systems as well.[55] Control loops enable simple motor tasks like taking a sip of water as well as complex organizational tasks like choosing targets in attack to achieve a military objective. Routines, habits, standard operating procedures, corporate rituals, and "battle rhythms" are all basic

---

[54] *Ibid.*, 65-116

[55] Karl W. Deutsch, *The Nerves of Government: Models of Political Communication and Control* (New York, NY: Free Press, 1966); John D. Steinbruner, *The Cybernetic Theory of Decision: New Dimensions of Political Analysis* (Princeton, NJ: Princeton University Press, 1974); Herbert A. Simon, "Applying Information Technology to Organization Design," *Public Administration Review* vol. 33, no. 3 (1973): 268-278; James G. March and Herbert A. Simon, *Organizations* (New York, NY: Wiley, 1958); James R. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge, MA: Harvard University Press, 1986). The basic theoretical statement is Norbert Weiner, *Cybernetics or Control and Communication in the Animal and the Machine* (Cambridge, MA: MIT Press, 1965). For the origins of the idea see Jean-Pierre Dupuy, *The Mechanization of the Mind: On the Origins of Cognitive Science* (Princeton, NJ: Princeton University Press, 2000); Mindell, *Between Human and Machine*. For a critique from the sociology of scientific knowledge perspective, see Geoffrey C. Bowker, "How to Be Universal: Some Cybernetic Strategies, 1943-70," *Social Studies of Science* vol. 23, no. 1 (1993): 107-127. Hutchins' concept of distributed cognition certainly draws on the cybernetic tradition.

features of organizational life.[56] As Clausewitz notes that routines are useful for "reducing natural friction and easing the working of the machine."[57] Software applications, likewise, consist of millions of interlocking control cycles, and the basic vocabulary of computer science is distinctly bureaucratic: "programs" are ordered sets of conditional "rules" arranged in "procedures," "functions," "routines" and "methods," while "code" follows "protocols" and writes to "registries."[58] Computers lack judgment in the performance of their routines, no matter how many supplementary routines are piled on to enable them to fake it.[59] In contrast, people often pay conscious attention to and adjust the performance of their control cycles.[60] Even an activity as mundane as climbing a ladder involves ongoing compensation for the ladder's movement.[61] Because people have discretion (slack time, space, or resources) to vary routine performances, routines actually become resources for change and adaptation.[62] When heedful

---

[56] For a thorough review of the concept of routine in organization theory see Markus C. Becker, "Organizational Routines: A Review of the Literature," *Industrial and Corporate Change* vol. 13, no. 4 (2004): 643-678. See also, *inter alia*, Herbert A. Simon, *Administrative Behavior, 4th Edition* (New York: Free Press, 1997); Steinbruner, *Cybernetic Theory*; Richard R. Nelson and Sidney G. Winter, *Evolutionary Theory of Economic Change* (Cambridge, MA: Belknap Press, 1982); Brian T. Pentland and Martha S. Feldman, "Organizational Routines as a Unit of Analysis," *Industrial and Corporate Change* vol. 14 (2005): 793-815.

[57] *On War*, 153.

[58] Jon Agar, *The Government Machine: A Revolutionary History of the Computer* (Cambridge, MA: MIT Press, 2003) emphasizes the governmental origins of computation, as contrasted with the corporate origins emphasized by Alfred D. Chandler and James W. Cortada, *A Nation Transformed By Information: How Information Has Shaped the United States From Colonial Times to the Present* (New York, NY: Oxford University Press, 2003); Joanne Yates, *Control Through Communication: The Rise of System in American Management* (Baltimore, MD: Johns Hopkins University Press, 1993). Early "computers" were women who tabulated data in huge work-centers; Jennifer S Light, "When Computers Were Women," *Technology and Culture* vol. 40, no. 3 (1999): 455-83.

[59] When one types "2+2" into a calculator, it displays "4" without any understanding of summation. If it displayed "5" only a human observer would recognize that it was the "wrong" content, unless the machine also included rules to detect the error by comparing some other formal symbols, which just pushes the semantic problem up a level. A good interface is supposed to anticipate the user's needs, but that "user illusion" ultimately depends on the developer's best guess of probable use case scenarios, expressed as a set of logical branches and sequels. This gets at an essential problem in the philosophy of mind. At some point human intentional content must depend on physiological processes. If it's possible for a physical brain to cause human consciousness, then where is the line drawn between machines simulating mind-like performances and their actually having mind-like properties? Is there a real difference between stupid computers and smart humans, or is the mind just a particularly clever program designed by evolution? See Daniel C. Dennett, *Consciousness Explained* (Boston, MA: Little, Brown and Co., 1991).

[60] Brian Cantwell Smith, *On the Origin of Objects* (Cambridge, MA: MIT Press, 1996), 191-212.

[61] Gilbert Ryle, "Improvisation," *Mind* vol. 85, no. 3 (1976): 69-83, argues that improvisation "is not something that is peculiar to a few distinguished persons, but something that is shared in very different degrees, in very different forms, and with very variable frequencies by all non-infantile, non-retarded, non-comatose human beings." (p. 69). Some bureaucrats seem to meet those conditions, but nonetheless, the point is that some degree of change and improvisation is required simply to do "the same thing" reliably.

[62] Wanda J. Orlikowski, "Improvising Organizational Transformation Over Time: A Situated Change Perspective," *Information Systems Research* vol. 7, no. 1 (1996): 63-93; Martha S. Feldman, "A Performative Perspective on

performance breaks down and humans just mindlessly execute algorithms, however, the potential for accidents soars.[63] Organizational information systems consist of loops within loops, complementarily performed by both human and machines.

Any control cycle, whether mindful or mindless, has three phases. In *perception*, sensors measure the state of the world. In *integration*, internal controls compare this to a goal state and measure the difference. In *articulation*, effectors take action to bring them into alignment. *Feedback* starts the process over again. As Hutchins notes of the navigational fix cycle, any control loop "is truly a cycle of activity, with no unambiguous beginning or end. Each step depends on a previous step and feeds subsequent steps."[64] The phases are analytically useful in showing how we can move from the physical state of a battlefield full of people and vehicles to the tidy little representations on *PowerPoint* slides that officers obsessively update. Figure 3-3 depicts an anti-aircraft battery as a simple example of distributed cognition with humans and machines performing all the phases of control: "A tracking device (optical or radar) follows the target; the computer calculates its speed and direction, and then extrapolates that velocity into the future to choose an aiming point for the guns. A ballistics calculation turns this information into angles of elevation and azimuth for the guns."[65] Obviously control of entire militaries is terrifically more complex, but it is built up out of the same sort of loops within loops.

Stability and Change in Organizational Routines," *Industrial and Corporate Change* vol. 12, no. 4 (2003): 727-752. Becker, "Organizational Routines," describes a divide between scholars who see routines as mindless repetition versus those who emphasize effortful accomplishment and notes that "it largely runs along the line of conceptual vs. empirical work. All the references cited above for the first camp are to conceptual papers, while the references cited for the second camp are empirical papers. These latter...[show] how, in a variety of organizations, such as call centers, information technology firms, small firms and housing organizations, routines are characterized by being changeable and open to variation." (p. 648)

[63] Karl E. Weick and Karlene H. Roberts, "Collective Mind in Organizations: Heedful Interrelating on Flight Decks," *Administrative Science Quarterly* vol. 38, no. 3 (1993): 357-81

[64] Hutchins, *Cognition in the Wild*, 133

[65] David A. Mindell, "Automation's Finest Hour: Radar and System Integration in World War II," in *Systems, Experts, and Computers: The Systems Approach in Management and Engineering, World War II and After*, ed. Agatha C. Hughes, and Thomas P. Hughes (The MIT Press, 2000), 34 (Figure 1.4 and caption)

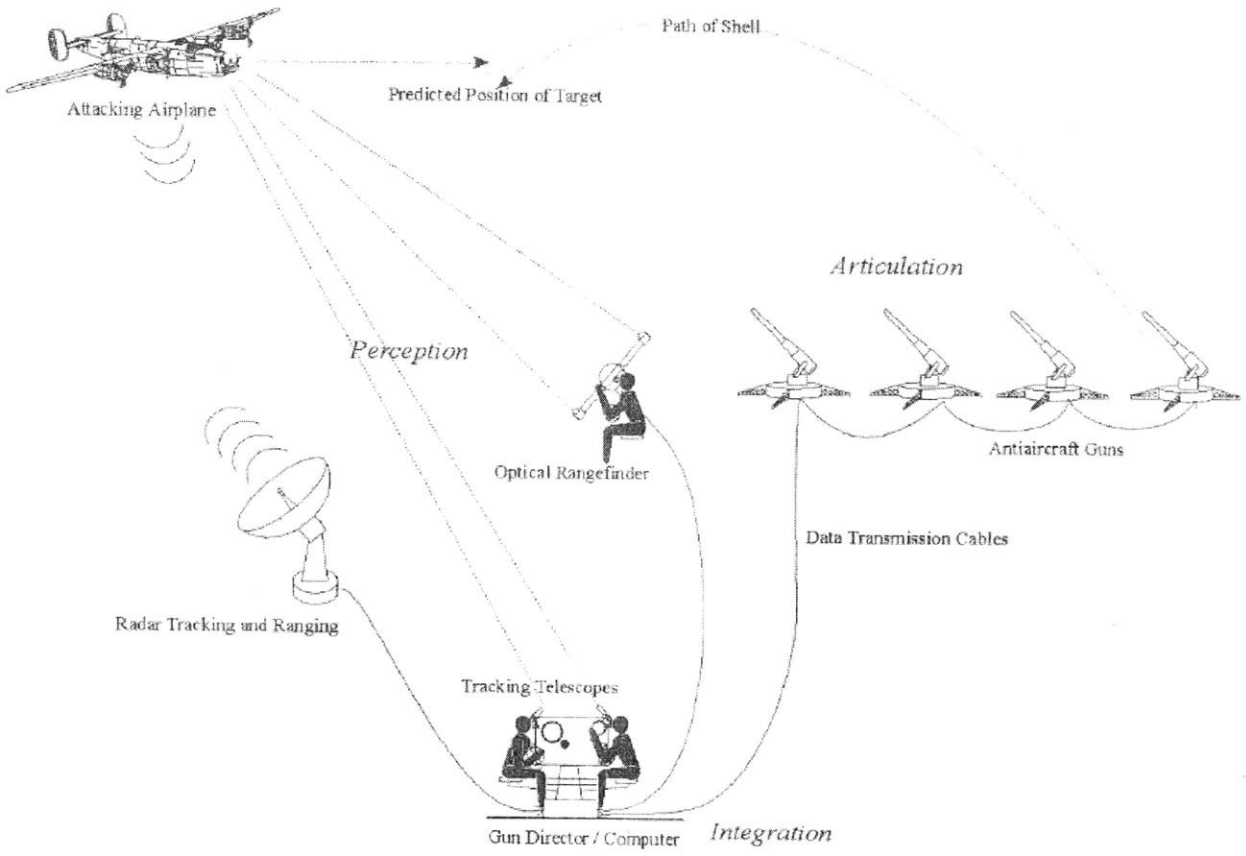


Figure 3-3: The antiaircraft problem, showing the three phases of control (D. Mindell)

3.3.2.3 Command and Control Doctrine

Before I step through each of these three phases in depth, I must mention the prominent role of the control cycle in military doctrine. I will illustrate the organizational problem of defining the computational goal of the control cycle and provide an example of a more complex control loop than pictured in Figure 3-3. U.S. doctrine holds that victory goes to the fastest control cycle: "Conceptually, the ability to process information into action via the cycle at a quicker pace than the opposition can be thought of as getting 'inside' the adversary's decision cycle by making the friendly force cycle smaller than the opponent's."[66] Unfortunately, high information friction causes control loops to run either too slowly or, more perniciously, too quickly after the wrong sorts of targets. Sometimes it's better to wait for an opponent to make a mistake or exhaust himself before doing something rash.

---

[66] U.S. Joint Chiefs of Staff, *Joint Publication 3-13.1: Joint Doctrine for Command and Control Warfare* (Washington DC: Government Printing Office, 1996), A-1

U.S. doctrine is replete with stylized feedback loops (Figure 3-4). Such models call practitioners' attention to features of their collective performance and orient them to the bureaucratic format which makes military content available. They can facilitate mindful performance of routines, collective sensemaking with colleagues, and standardization of best practices.

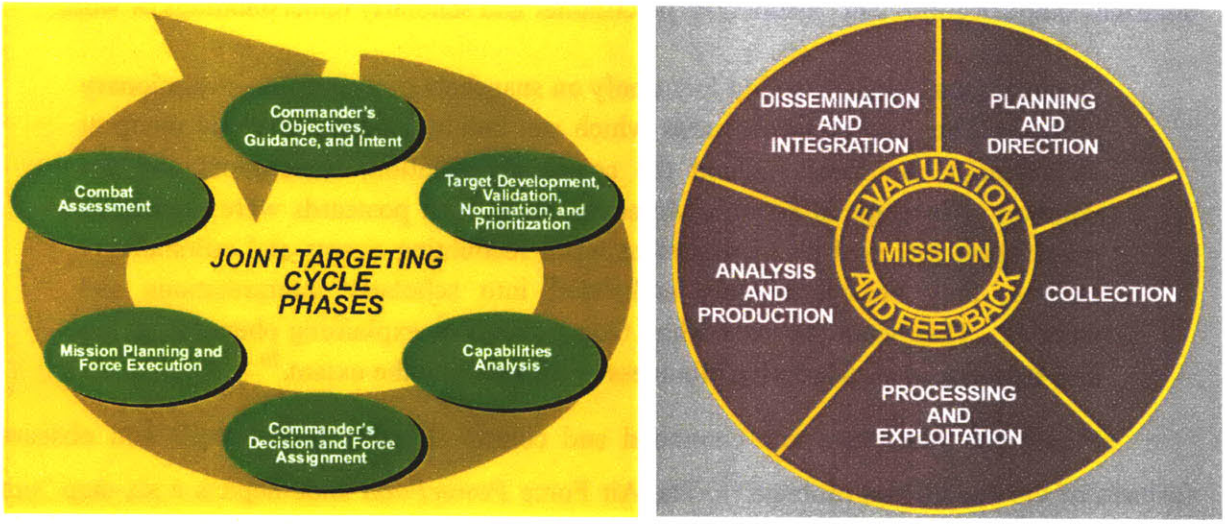


Figure 3-4: The Targeting Cycle and the Intelligence Cycle in U.S. doctrine.[67]

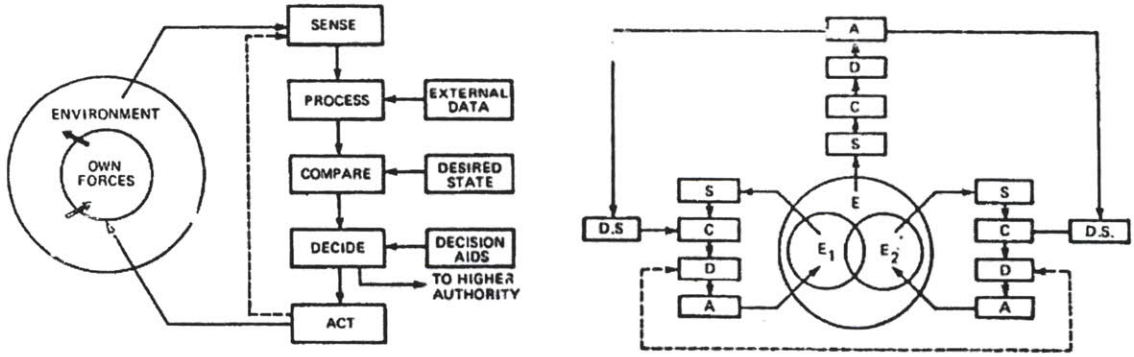


Figure 3-5: Command and control as feedback (left) with overlapping and nested control (right)[68]

However, such models can be profoundly misleading in what they leave out. Technocratic models of command and control like Figure 3-5 bottle up commanders in clinical

[67] U.S. Joint Chiefs of Staff, *Joint Publication 3-60: Joint Doctrine for Targeting* (Washington DC: Government Printing Office, 2002), II-3, and *Joint Publication 2-0: Doctrine for Intelligence Support to Joint Operations* (2000), vi.
[68] Joel Lawson, Jr., "Command Control as a Process," *IEEE Control Systems Magazine* vol. 1, no. 1 (1981): 5- 11

decision nodes.[69] Unfortunately, when information friction is high, however, then "desired states" are politicized, "decision aids" are used rhetorically rather than functionally, and the data processing connecting "sense" to "act" is frustrated by breakdowns, fatigue, anger and noise. Doctrinal accounts leave out the situated context of command and control and the political processes of sensemaking. Management ethnographer Claudio Ciborra points out that such doctrinal simplifications can corrupt both practitioner and scholarly understandings of work:

> Organizational models tend to focus only on snapshots of a complex, evolutionary process...They represent postcards which can barely capture, let alone interpret and explain, the forces behind the constant e-volution, re-volution, and de-volution of managerial action. Moreover, since such postcards were repeatedly relied upon and used by management when recounting events and rationalizing choices, they became silently embedded into scholarly interpretations and theories...They were retrieved when facing events or explaining phenomena, but also reproduced a self-sealing blindness to the new and the extant.[70]

Figure 3-6 illustrates how command and control doctrine both reveals and obscures features of the operational problem.[71] The Air Force *PowerPoint* slide depicts a six-step "time critical targeting" cycle, also known as the "kill chain."[72] Using the terminology introduced above, *perception* occurs in the "find" step, integration in "fix" and "track," *articulation* in "target" and "engage," and ongoing *feedback* in "assess." A variety of distributed reconnaissance

---

[69] Thomas P. Coakley, *Command and Control for War and Peace* (Washington DC: National Defense University Press, 1992), 98-101

[70] Claudio Ciborra, *The Labyrinths of Information: Challenging the Wisdom of Systems* (New York, NY: Oxford University Press, 2002), 175. Ciborra's critical description of management science also applies to the military command and control community: "Disciplines such as ours that are inspired by the paradigm of the Galilean method [abstraction, formalization, arithmetization] tend to disregard the fundamental role of the everyday life world of the agents, users, designers and managers, and the messiness and situatedness of their acting, while privileging the geometric worlds created by system methodologies. In this way, the key element is neglected: human existence, which represents the essential ingredient of what information is, of how the life world gets encountered, defined, and reshuffled" (p. 18).

[71] Brig Gen Jim Morehouse, "Time Critical Targeting," Presentation at National Defense Industrial Association DoD Interoperability Conference (26 March 2002), http://www.dtic.mil/ndia/2002interop/morehouse.pdf [accessed 10 July 2009].

[72] In 1996 Air Force Chief of Staff General Ronald Fogleman declared, "In the first quarter of the 21st century, it will become possible to find, fix or track, and target anything that moves on the surface of the Earth"; John A. Tirpak, "Find, Fix, Track, Target, Engage, Assess," *Air Force Magazine* vol. 83, no. 7 (2000). The U.S. military has a penchant for borrowing vocabulary from the business world. The "kill chain" is an analogy to the global "supply chain." Intelligence sections deliver target data to their "customers" so that bombers can "service the target." Note also the Air Force logo and "Integrity-Service-Excellence" motto which provide corporate branding. At the very least this illustrates the convergence of military and business administration cultures, to say nothing of whether this makes good normative sense for the administration of violence.

and strike platforms, together with various data processing systems, all work on different and partial information problems.

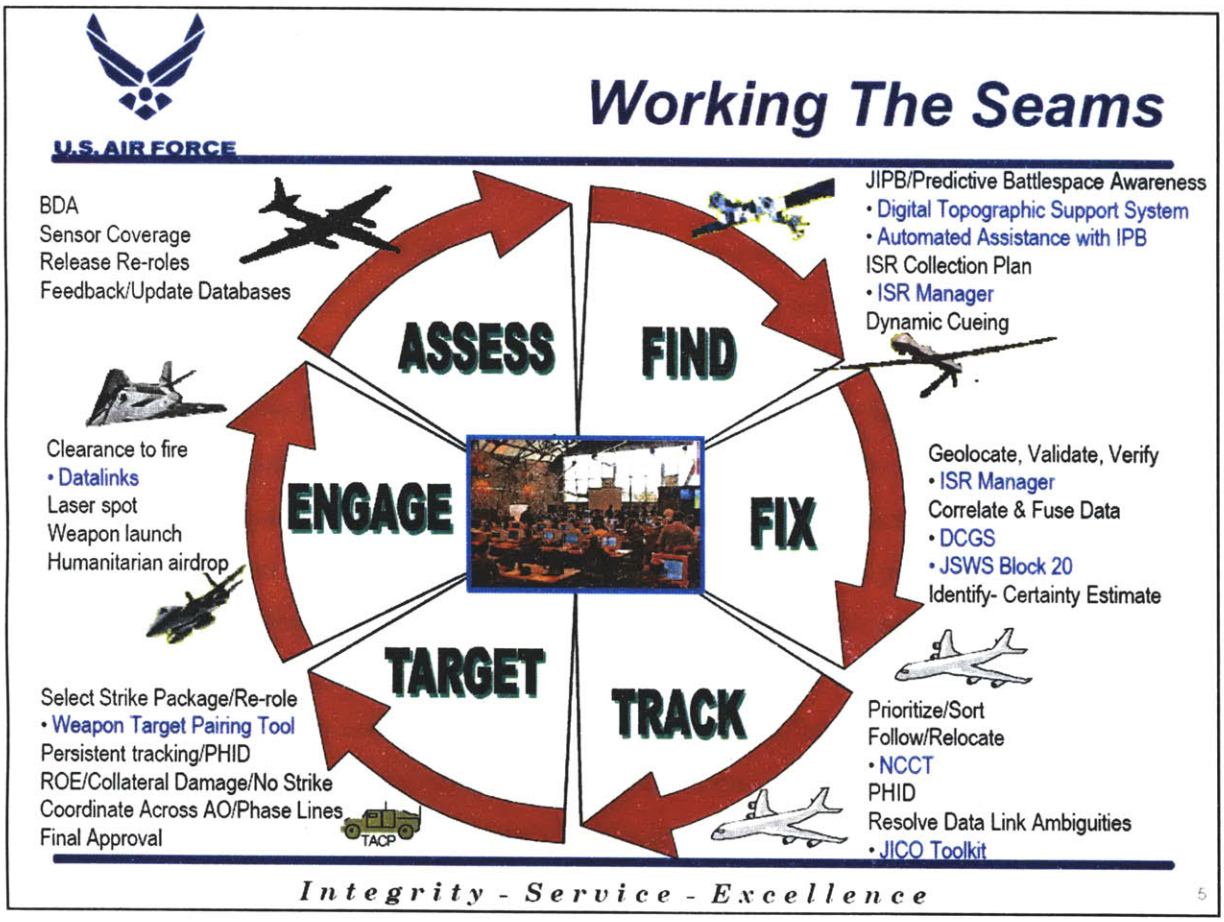


Figure 3-6: Air Force implementation of time critical targeting in 2002

At the center is an Aerospace Operations Center (AOC). In a testament to the contemporary weaponization of information, the Air Force has designated the AOC as a programmatic "weapon system" in its own right, even though it is nothing but a room full of people and computers.[73] The slide title, "Working the Seams," calls attention to all the representational transformations throughout the "kill cycle" which limit its efficiency. Unlike most doctrinal depictions of rational control loops like Figure 3-5, instead Figure 3-6

[73] AOC operations are detailed in: Michael W. Kometer, *Command in Air War: Centralized Versus Decentralized Control of Combat Airpower* (Maxwell AL: Air University Press, 2007). On the AOC as weapon system: Ruth Liebowitz, *Acquiring the Air and Space Operations Center: The AOC WS System Program Office, a Short History 2000-2003* (Hanscom Air Force Base, MA: Air Force Electronic Systems Center, 2006). The AOC contrasts with more distributed and *ad hoc* historical implementations of CAS: Benjamin Franklin Cooling, *Case Studies in the Development of Close Air Support* (Washington, DC: *Office* of Air Force History, 1990)

interestingly highlights the distributed struggle to deal with all information friction generated in complex distributed cognition. Airmen have to pay attention not only to targets and aircraft (information content), but also to computer systems, data links, and communication protocols (information format). One way to help them do so is via meta-representations like this slide, which represents representational processes. Figure 3-6 helps airmen to see the sociotechnical problems they must debug in order to command and control the air war.

Nowhere on the slide, however, is there mention of targeting objectives. This slide focuses attention on running the kill chain faster and more reliably, but it takes for granted that targets exist *as* targets. Technical problems of tracking and prosecuting targets complicated, but nevertheless, well-defined. When questions of *why* one is targeting and what *effect* one hopes to achieve are passed over in the rush to debug a complex machine, then targeting can become an end in itself.[74] The operational problems of running a campaign become hijacked by the tactical problems of prosecuting targets, displacing attention from important targets (and important targets to avoid) to those which are *merely available.* By 2003, the "kill chain" had become a generalized metaphor across the services for "servicing" mobile targets, to include individual insurgents. This organizational conveyer-belt loads up targets and processes them, "sensor to shooter," concentrating on engineering a reliable general-purpose machine.[75] Exclusive attention to debugging the representational means displaces consideration of computational ends. Table 3-4 summarizes information friction at the systemic level in distributed cognition.

Table 3-4: Systemic information friction in distributed cognition

	Low Information Friction	High Information Friction
• Computational Goals	Defined/shared	Ambiguous/controversial
• Representation	Efficient	Ends-means misalignment
• Routine Performance	Heedful interrelating	Mindless execution
• Command and Control Doctrine	Orients practitioners to bureaucratic format	Simplistic expulsion of messy realities

[74] The targeting cycle is only one heuristic that personnel use to make sense of and describe more complicated operations. Another related framework which generalizes on targeting is so-called "Effects Based Operations" wherein a careful consideration of desired (and undesired) first and second order effects are supposed to drive operational options, which may not be exclusively "kinetic" destruction; see Edward A. Smith, *Effects Based Operations* (Washington D.C.: Department of Defense CCRP Publications Series, 2003). Any metarepresention both reveals and obscures features of the problem.

[75] *E.g.*, "Accelerating the Kill Chain: Closing the Sensor-to-Shooter Cycle" in "The Challenges of Command and Control in Urban Operations," *Defense Update* no. 1 (2006).

3.3.3 Perception

We now move on to a description of information friction in each of the phases of the control cycle. In the perception phase of control, sensors make physical contact with the environment and create records of the event. Perception parses William James' "great blooming, buzzing confusion"[76] into distinct symbols. The battlefield is what it is, full of men and material bumping and shoving each other. Measurement devices exploit some physical relationship to an aspect of this situation. The resultant state of those devices can be transformed into symbolic records by constrained operations which preserve reference to the state of the world. Records can be moved to a disconnected place where they can be freely manipulated and combined in order to clearly emphasize some features of the world. Perception is a series of choices that structure and amplify features of the world. For the same reason it necessarily suppresses some features in order to discriminate others.

3.3.3.1 Cascades of Inscription

"What lies between the problem and its solution?," Hutchins points out, "Between the relationship of the ship to its environment and the position plotted on the chart lie a number of representational media across which the representations of the spatial relationship of the ship to the world are propagated."[77] Each transformation along the circuit sets up the material context of the next step, which constrains the way actors interpret their situation and then set up further steps for others (or for themselves later in time). Representations of the world propagate through the system via constrained transformations which preserve reference to regularities in the environment. Bruno Latour describes this process as a "cascade of inscription," with an emphasis on the institutional work required to structure representation.[78] Military officers as well as scientists "start seeing something once they stop looking at nature and look exclusively and obsessively at prints and flat inscriptions. In the debates around perception, what is always forgotten is this simple drift from watching confusing three-dimensional objects, to inspecting

---

[76] William James, *Principles of Psychology* (Henry Holt & Co., 1890), 488

[77] Hutchins, *Cognition in the Wild*, 119

[78] Latour, *Science in Action*. He uses "circulating reference" for the same idea in *idem*, *Pandora's Hope: Essays on the Reality of Science Studies* (Cambridge, MA: Harvard University Press, 1999), Chapter 3. Latour's notion of "immutable mobile" inscriptions compares well with Hutchins' discussion of durable representational media which preserve environmental invariance.

two-dimensional images which have been *made less confusing*."[79] The alignment of cascades is a matter of ongoing effort and potential controversy among participants.

When information friction is high, cascades are corrupted. Unconstrained transformations or unaccounted degrees of freedom undermine the relationships between representations. Signals become hard to pick out of the noise, and equivocation mounts for those symbols which are produced. Actors seek to wrest control of information flows, preferentially emphasizing some features and suppressing others, or denying access altogether. They may channel, restrict, or redirect cascades, or even intentionally introduce deception or exaggeration into them in order to further their interests.

3.3.3.2 Referential Integrity

A basic question about any piece of military information is whether or not it's true. As long as all of the transformations in the cascade stand in some constrained relationship to one other, then it will usually be possible to map them back onto the state of the world. If that relationship is poorly constrained, however, then symbols drift away from reality. As an American intelligence analyst who tracked Soviet submarines at Fleet Ocean Surveillance Information Center (FOSIC) London in 1986 recalls, "I noticed that the intelligence plot begins to assume a reality of its own. During a crisis, it is sometimes difficult to separate the real action from the action 'manufactured' by the intelligence center. *One tends to get caught up in the 'truth' of the technological representation*...Occasionally, a unit described in reports as having 'probably returned to port' had only fallen off the map after losing magnetism."[80] Referential integrity was compromised—the submarine plot was false—but nobody knew the difference until they found the token for the "lost" submarine lying on the ground.

Ultimately, the truth of any representation is only tested through the action it enables. If surprises and inconsistencies emerge, then we suspect information is false. Yet until that pragmatic loop closes, a representation remains an open hypothesis. Actors can only have faith that the cascade keeps representations pointing in the right direction, as James observes:

---

[79] Bruno Latour, "Drawing Things Together," in Michael Lynch, and Steve Woolgar, Ed., *Representation in Scientific Practice* (Cambridge, MA: MIT Press, 1990), 39 (italics in original). Latour notes that actor-network theory focuses on the processes which transform "rats and chemicals into paper" (22).

[80] Alexander P. Butterfield, "The Accuracy of Intelligence Assessment: Bias, Perception, and Judgment in Analysis and Decision," Naval War College Paper (March 1993), 4-5 (emphasis added)

> Truth lives, in fact, for the most part on a credit system. Our thoughts and beliefs 'pass,' so long as nothing challenges them, just as bank-notes pass so long as nobody refuses them. But this all points to direct face-to-face verifications somewhere, without which the fabric of truth collapses like a financial system with no cash-basis whatever. You accept my verification of one thing, I yours of another. We trade on each other's truth. But beliefs verified concretely by somebody are the posts of the whole superstructure.[81]

When information friction is high, then personnel trade representations that may be counterfeit, worthless, or otherwise irredeemable. Referential integrity is compromised when no path of constrained transformations links a symbol back to a situation on the battlefield without surprise or disappointment. James notes, "Experience, as we know, has ways of boiling over, and making us correct our present formulas."[82]

Referential integrity is not inherent in a symbol. It is a relational property between a token, its context of interpretation, and the state of the world. When a symbol is taken out of context, referential integrity can break. During the First World War the British Admiralty operated direction finding stations to monitor the radio traffic of the German High Sea Fleet. On 31 May 1916, the Director of the Admiralty's Operations Division asked his cryptologic center, Room 40, where the stations placed the radio call sign "DK." They told him that it was in port at Wilhelmshaven. Room 40 personnel knew well that the German Admiral Scheer transferred "DK" ashore and assumed a different call sign at sea, but the Director asked about "DK" and did not explicitly ask for Scheer's whereabouts. The Director proceeded to signal the British Admiral Jellicoe that the German fleet had not yet left port. Jellicoe was surprised indeed to find himself four hours later confronting the entire High Sea Fleet in the close-run and inconclusive Battle of Jutland. Jellicoe afterward tried to pursue the battered Germans (the whole battle was the first major naval engagement to take place beyond visual range), but when Room 40 passed him an intercepted position reported from a German ship, it turned out that the ship's faulty navigation had reported its own position incorrectly. These two errors shattered Jellicoe's confidence in Room 40, and so he ignored later intercepts that actually indicted the correct position and heading of the Germans. Jellicoe sailed off in the opposite direction, and Scheer

---

[81] William James, *The Writings of William James: A Comprehensive Edition*, ed. John J. McDermott, (Chicago: University of Chicago Press, 1977), 433

[82] *Ibid.*, 438

escaped. In each case, the truth of any particular piece of information depended on the context of interpretation. "DK" was taken out of a perfectly good cascade and inserted into another which cued inappropriate action; true information was falsified. The ship with the bad navigation reports undermined the intelligence-operations cascade from the get-go; false information was incorrectly validated. The reports that finally did maintain referential integrity were worthless because Jellicoe refused to trade on their value; true information was unperceivable.[83]

To fill out the logical possibilities, false information might be rendered true with a bit of luck and creative interpretation. After the 1797 battle of Cape St. Vincent, Admiral Sir John Jervis came under some criticism for having failed to make a signal which might have brought a rout of the Spanish fleet rather than the nominal victory it turned out to be. Upon first contact, the English and numerically superior Spanish sailed in opposite directions. Jervis signaled his van—the head of his line—to tack and successfully broke through the Spanish line, but the van was considerably outgunned. The rest of Jervis's line waited to tack in succession and missed the action. The counterfactual criticism from the Admiralty was that Jervis should have signaled the rear of his fleet to wear in order to double the Spanish line.[84] However, Jervis was in fact constrained by the Royal Navy signal book, which did not have a proper signal for the specific situation in which Jervis found himself. Jervis may in fact have attempted to signal his intent to wear using two different and confusing signals, but in the smoke and noise they were misunderstood by every captain, with the important exception of Horatio Nelson aboard *HMS Captain*. Nelson wore to join the outnumbered and outgunned English van, and helped to deliver an improbable victory against the Spanish.[85] Nelson made a bad signal good with a mix of literal disobedience of the flags and Clausewitzian *coup d'oeil* in the particular circumstances.[86]

---

[83] Patrick Beesley, *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Center 1939-1945* (London: Greenhill Books, 2000), 3-4; Michael A. Palmer, *Command At Sea: Naval Command and Control Since the Sixteenth Century* (Cambridge, MA: Harvard University Press, 2005), 242-250

[84] To wear is to fall off from the wind and come up close-hauled in the other direction, the opposite of tacking. To double the line is to sail two lines of warships on either side of the enemy line in order to attack from both sides.

[85] Michael A. Palmer, *Command at Sea: Naval Command and Control since the Sixteenth Century* (Cambridge, MA: Harvard University Press, 2005), 170-177.

[86] Clausewitz, *On War*, 102: "During an operation decisions have to be made at once: there may be no time to review the situation or even to think it through... If the mind is to emerge unscathed from this relentless struggle with the unforeseen, two qualities are indispensable: *first, an intellect that, even in the darkest hour, retains some glimmerings of the inner light which leads to truth; and second, the courage to follow this faint light wherever it*

In a more famous and more decisive act of disobedience during the 1801 Battle of Copenhagen, Nelson "turned a blind eye" to Admiral Sir Hyde Parker's signal to withdraw and instead flew his own signal for close battle. Nelson's squadron then mauled the Danish-Norwegian fleet and scored an important strategic victory.[87] Such outright disregard or alteration of signals—by shutting off radios or tampering with email—remains one sure way to break a cascade of dubious referential value, and is no doubt practiced more frequently in modern militaries than technocratic accounts of command and control appreciate. Obviously the consequences of intentional non-communication might not always be as fortuitous as Nelson realized. Nelson's cases are interesting examples of internal self correction within a system beset with high information friction.

Representations of the world are quite literally constructed by people and machines. The construction may be flimsy or robust, and actors who take it on faith—as they must—can find themselves quite unpleasantly surprised when they find their assumptions violated. Referential integrity is the reliable coordination between the state of a representation and the state of the world, but this reliability can only be finally tested in action. James writes, "Truth *happens* to an idea. It *becomes* true, is *made* true by events."[88]

3.3.3.3 Provenance

Testing referential integrity in battle is obviously costly. If it is possible to inspect the construction of facts in advance, then one can gain more confidence whether they are reliable. Provenance is the origin of a work of art or artifact: time, place, artist, *etc.* To determine provenance, which is essential in determining whether an artwork is genuine or a forgery, art historians follow sales or shipping records and critical mentions that link the present owners to

---

may lead. The first of these qualities is described by the French term, *coup d'oeil*; the second is *determination*." (italics in original)

[87] Palmer, *Ibid*, 191, describes not only deliberate disobedience of the order, but also deliberate deception of Parker to ensure that Nelson's countervailing order was carried out: "Nelson grabbed a glass and turned to his flag captain, Thomas Foley...'You know, Foley,' he said, 'I have only one eye—and I have a right to be blind sometimes.' Placing the glass to his blind eye, he exclaimed: 'I really do not see the signal!' Satisfied, he told anyone within earshot: 'Damn the signal. Keep mine for close battle flying. That's the way I answer such signals! Nail mine to the mast!'...most of [Nelson's] captains remained in place, and in the fight. Graves, who as a flag officer was duty bound to repeat the signal, waited fifteen minutes and then flew [Parker's signal to withdraw]...from that point [where] the signal was visible to Parker['s flagship] but invisible to the other ships of the line to Grave's rear...Graves had no intention of withdrawing and, like Nelson, kept the signal for close action flying from the main. But his acknowledgement was visible...Had Nelson's squadron heeded Parker's signal, disaster would certainly have followed."

[88] "The Meaning of Truth" in *Writings of William James*

the original artist, along with other cues in the artwork itself such as the artist's style and the physical properties of aging paint on canvas. Most criminal justice systems similarly require a written chain of custody to prevent evidence tampering. Provenance is a historical fact about an item, but it can only be surmised through evidence which indicates its origin.

In the case of data, explicit evidence of provenance or *metadata* is the same type of thing as that to which it refers. Each piece of evidence is itself only another representation subject to the same concerns about representational integrity. We judge them based on their number and relationship to one another. As items of metadata accumulate in number and diversity without appearing inconsistent, then our confidence increases in the authenticity of the item to which they refer. The judgment stands on a system of references, not any inherent property of the symbols.

Many representational genres explicitly include metadata such as the date of creation and modification, the author, validating organization, security classification, *etc.*, but the actual relationship of data and metadata can be ambiguous. Hardcopy paper representations include some inherent provenance clues in the condition of the paper, official seals, or handwriting. By contrast, the association of metadata with digital products is far more arbitrary. Sourcing data is easily stripped away in a cut-and-paste operation. Any metadata that has to be explicitly populated by the author takes time away from working on the data itself, which can either slow down production or lead to the disregard of metadata fields altogether. Software programs can automatically populate some metadata, such as the date of file creation. Yet this can be misleading if, for example, this date refers to creation of a *copy* of the file rather than creation of the content of the file. Some database systems automatically populate metadata fields with default values, which can be mistaken for considered values by casual users at a later time (as often happens with zero—"0"—in numeric fields if there is no allowance to represent "null" or "no measurement").

Military information has an additional provenance challenge because of security classifications. Information to identify intelligence sources and methods is often intentionally stripped or "sanitized" in reports that go out to consumers. For example, sensitive signals intelligence might be worded to appear as if it could have plausibly been provided by a human spy. This might have the unintended consequence of making solid intelligence seem less reliable

to commanders used to distrusting spies, as in fact happened with Allied Ultra intelligence on a number of occasions in World War II. Reflexive overclassification is another problem, caused by personnel assigning the highest possible classification to their documents to avoid accidentally disclosing something. Correctives such as paragraph-level classification markings require substantially more time to implement reliably, with no guarantee that the appearance of meticulous classification really corresponds to the "real" source of the data.

When information friction is high, then metadata is missing, misleading, or just wrong. Provenance clues are unreliable or unavailable; therefore, the provenance of data is unascertainable. Personnel who act on such information have little insight into the context of its production. The absence of provenance can conceal data-processing mistakes, inadvertent distortions, intentional lies by bureaucratic competitors, and enemy manipulation. It becomes impossible to confidently answer the question, "Why do you trust that information?"

Table 3-5 sums up manifestations of information friction in the perception phase.

Table 3-5: Information Friction in Perception

	Low Information Friction	High Information Friction
• Cascades of inscription	Constrained transformations	Corrupted, noisy
• Referential integrity	Preserved	Equivocal
• Provenance	Recorded & reliable	Unkown

3.3.4 Integration

Integration is the knowledge management phase of the control cycle. It "performs a kind of translation, from perception to articulation,"[89] by comparing and combining multiple information cascades with one another and with information in memory. The combination produces new refined information to enable commanders to exert downstream control. Commanders gather around abstract maps and graphs in order to make sense of the state of the world and to figure out how they would like to intervene in it in order to change it and to bring it closer into alignment with their mission objectives.

[89] Mindell, *Between Human and Machine*, 23

3.3.4.1 Centers of Calculation

Sand tables of battlefield terrain, submarine plotting boards, and command centers festooned with plasma screens are all spaces for performing integration. Latour refers to the confluence of inscription cascades as *centers of calculation.* Centers facilitate the combination of inputs into authoritative maps or databases. Miniature models of the outside world enable personnel to gather around and observe it all in one place. They provide state-based memory, which means that updates accumulate over time into a central location where they can be viewed all-at-once (or quickly replayed). Paul Edwards uses the metaphor of the "closed world" to describe military centers of calculation;[90] while his phrase evokes insulation from reality, the principle liability of such centers, it also understates the degree to which centers are actually open to incoming and outgoing cascades. Indeed, the reason that centers work at all is because they have the freedom to rearrange symbolic representations disconnected from the world in order to then articulate some later reconnection to it.

The U.S. Pacific Fleet's official history in 1945 noted, "Collation is the heart and soul of intelligence."[91] A CIA officer in Vietnam describes "the card catalog cases expanding along the walls of the data trailer...documenting [Viet Cong] units' complete order of battle, identifying almost all the officers and men." He highlights the power of organized records to establish a connection to entities separated in space and time, observing that "in much of the infamous Iron Triangle we had turned an invisible enemy into a visible one."[92] Such tools enable analysts to gather records of events separated widely in space and time into consolidated pictures of reality.

Rodger Winn in the Royal Navy's Operational Intelligence Center (OIC) during the Second World War called his submarine tracking plots a "working fiction." The room received radio direction finding reports, Ultra signals intelligence from Bletchley Park, U-boat sightings from friendly patrol craft and airplanes, and reports of sinkings and convoy attacks. The OIC represented every known German U-boat with a pin with a unique two-letter code (AA, BB,

---

[90] Paul N. Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America* (Cambridge, MA: MIT Press, 1996)

[91] Cited in Christopher A. Ford and David A. Rosenberg, *The Admirals' Advantage: U.S. Navy Operational Intelligence in World War II and the Cold War* (Annapolis, MD: Naval Institute Press, 2005), 3

[92] Orrin DeForest and David Chanoff, *Slow Burn: The Rise and Bitter Fall of American Intelligence in Vietnam* (New York, NY: Simon & Schuster, 1990), 135. DeForest also laments that his databank was populated years too late and unable to make a difference to American forces fighting the invisible enemy with indiscriminate search and destroy tactics rather than more selective intelligence-guided targeting.

etc.). Analysts associated every report they received with a particular U-boat and estimated its position. Beesly describes the guesswork which built up the plot:

> The incidents themselves were penciled in on the chart so that, when something unexpected occurred that did not fit in with previous ideas, the whole process could be started afresh and the incidents formerly associated with one U-boat now allocated to another...Winn insisted on complete honesty and, no matter how involved and painstaking the process of re-estimating, fresh pins could not be added to the plot to account for awkward events, or old ones removed just because there had been no recent evidence to support that particular U-boat's presence...Despite all its errors and imperfections the plot did bear some relation to reality.[93]

Here we see the transformation of incoming data, constrained by reported coordinates or numbers, into pencil marks on the corresponding part of the chart. These marks are combined with the experience of the analysts and the existing state of the pins into a new estimated position for the pins. The analysts' intuitive judgment—a Clausewitzian *coup d'oeil* which saw patterns through the noise—itself formed a constraint on the probable patterns of U-boat behavior internalized through repeated experience. The "working fiction" thus constructed became the basis for routing convoys away from the German wolf packs. Winn noted that, "What could only be an estimate and a guess was to be taken as a fact and acted upon."[94] His goal was not to be perfect, but to be right more than half the time.

The construction of authoritative representations can be misleading, however. Sometimes the working fiction is a dangerous fiction. Hitler was famously obsessed with strategic maps of the continent which bore slight resemblance to the fighting on the ground, especially during the epic battles on the Eastern Front versus the Soviets.[95] The reasons behind Hitler's foolishly impulsive orders are many, but his eagerness to believe in simple two-dimensional pictures was one of them. Well into the information age on 2 July 1988, a U.S. Ticonderoga-class cruiser, built around the state-of-the-art Aegis fire-control system, fired on Iran Air Flight 655 and killed nearly three hundred civilians. The U.S.S. Vincennes was engaged in combat against Iranian gunboats when her electronic combat information center detected an

---

[93] Beesly, *Very Special Intelligence*, 114
[94] Butterfield, "Accuracy of Intelligence Assessment," 5
[95] John Keegan, *The Second World War* (New York: Viking, 1990), 402

approaching aircraft. Her operators misinterpreted the ascending Airbus for a descending F-14 fighter on an attack profile and failed to notice Flight 655 when they checked the published listing of commercial flights. Although the Aegis radar worked perfectly, the entire man-machine system failed because it was primed to discriminate U.S. from enemy aircraft and to facilitate rapid decision-making, not to calmly identify an innocent civilian airliner that happened to be approaching from the same country which had just sent gunboats to attack.[96] The changing context detached the center of calculation from its world.

Centers of calculation provide their inhabitants with a sense of mastery, but whether or not they actually achieve it depends on the cascades of inscription which connect them to the battlefield and the ways in which they combine them to create the reality the center manipulates. Latour thus describes power as a fragile mastery over a network of inscription:

> A man is never much more powerful than any other...[unless his] eye dominates records through which some sort of connections are established with millions of others...This domination, however, is not a given but a slow construction and it can be corroded, interrupted, or destroyed if the records, files, and figures are immobilized, made more mutable, less readable, less combinable, or unclear when displayed. In other words, the *scale* of an actor is not an absolute term but a relative one that varies with the ability to produce, capture, sum up, and interpret information about other places and times.[97]

When information friction is low, then centers house panoptic representations of the world that provide a god's eye view of the features that matter for operations.[98] The center is connected to reliable provenance, and the sound construction of its incoming cascades ensures referential integrity. Abstract electronic displays of icons of ships, airplanes, and tanks reliably correspond to the position of real vehicles in real time. Network diagrams of terrorists correspond to the actual social networks that coordinate terrorism. Far flung units can take for granted their "common operational picture" to coordinate behavior. The center has "information dominance" over large swaths of the battlefield.

---

[96] Gene I. Rochlin, *Trapped in the Net: The Unanticipated Consequences of Computerization* (Princeton, NJ: Princeton University Press, 1997), 156-168

[97] Latour, "Drawing Things Together," 56 (emphasis in orginal)

[98] Foucault famously uses the "panopticon" prison design by Jeremy Bentham, which allowed centrally-located guards to view all of the prisoners silhouetted in their cells along the circumference of the prison, as a general metaphor for state surveillance of society and societal internalization of state control. Michel Foucault, *Discipline and Punish: The Birth of the Prison* (New York: Vintage, 1995)

When information friction is high, however, the center becomes a hermetically-sealed chamber. Electronic icons track ghosts that don't exist or shadows of entities long departed. Pictures are neither common nor operational. Representations that seem clear are actually irrelevant, while the rest appear illegible. Representations become fragmented across different sites, each with a different picture of reality that they are unable or unwilling to combine. Any sense of mastery that the charts and graphs convey is illusory, yet personnel continue to update them in order to enhance the illusion. In high information friction, centers of calculation suffer referential disintegration; they are de-centered.

A particular challenge of digitization is the loss of a single material site for combination of cascades and for bodily interaction with a single material plot. Instead of the OIC's chart full of pushpin U-boats, now thousands of files and versions of files on hundreds of PC workstations contain multiple private realities. There are so many places to fuse representational products that they can never all find their way into a fused picture under the same eye. Modern IT can represent fantastic complexity, but still it has to be compiled by many users on many machines and viewed through the tiny portholes of many monitors. The profusion of IT causes new centers of calculation to bubble up within existing ones.

3.3.4.2 Layers of Abstractions

Integration is actually performed throughout the cascades of perception and articulation, so there are many intermediate centers of calculation. The spymaster perceives and articulates while meeting with his source. He then retires into his safehouse to type up reports, in which he combines his notes, his memories and prior reporting. Reports from many agents flow into an intelligence center, where they are further combined into multi-source products describing the atmospherics and important events in a situation map of the area. The outputs of the intelligence center become inputs to a "common operational picture" at a higher headquarters where commanders ponder their options. Each of these nested loops implements much more work than is perceived in its interface with high order loops.

Any center of calculation builds on several layers of abstraction that clean up the incoming cascades of inscription. Movement from the "blooming, buzzing confusion" of the real world to the air-conditioned authority of the "closed world" is facilitated by intermediate steps that progressively buffer out local noise and amplify signals in order to produce clean and

reliable symbols. Both software architectures and bureaucratic hierarchies feature layers of abstraction to clean up the world for the executive functions. If all is working right, they produce a clean symbolic output with reliable provenance and referential integrity. Any technique which renders aspects of local realities commensurable and comparable in a single representation reduces uncertainty and renders localities countable, controllable and taxable.[99]

Standardized interfaces enable a great deal of speed and flexibility in passing details on changing data across all the different centers of calculation and in comparing the gaps between world-states and goal-states. Flexibility and confidence, that is, as long as the standardized types are the only things that officers want to discuss. Each bureaucratic center which implements an abstract interface is something of a "black box" for the others that connect to it. An engineering "black box" reliably transforms inputs into outputs so that users don't need to know the details of the circuits inside; the use of the box is supposed to be agnostic as to its interior content except as reflected in its performance characteristics. The "black box" has become a central metaphor in the sociology of technology for scientific and technical facts which can be taken for granted only after the resolution of controversy and confusion around their emergence. The point is that black boxes can be opened again if the abstraction breaks or is challenged.[100]

In practice all non-trivial abstractions are "leaky." Some circumstances force people to pay attention to implementation details at lower levels of abstraction.[101] For example, mobile phones abstract away the implementation of telephony in particular cellular towers, but phone users have to pay attention to dead zones and arrange their conversations around them. "Can you hear me now?" is the sound of implementation breaking through the abstraction. Even though the software development community espouses an aesthetic for elegant code, programmers sometimes cut corners by exploiting the internals or byproducts of procedures to meet an immediate need in the exigencies of development and debugging. Moreover, powerful development tools with high-level abstractions lower the barriers to entry for user/programmers who have not been socialized into the standards of sound computer science. They leave little documentary trail. A*d hoc* "spaghetti code" connects different procedures in confusing and

[99] Wendy Nelson Espeland and Mitchell L. Stevens, "Commensuration as a Social Process," *Annual Review of Sociology* vol. 24 (1998): 313-343; Bowker and Starr, *Sorting Things Out.*
[100] MacKenzie, *Inventing Accuracy*
[101] Joel Spolsky, "The Law of Leaky Abstractions," Joel on Software blog, 11 November 2002, http://www.joelonsoftware.com/articles/LeakyAbstractions.html

historically contingent ways. Runtime interdependencies become opaque and unpredictable in changing contexts. Over time, software architectures build up around legacy code in ways that are difficult to trace, understand, or represent in system diagrams. Technologies that don't behave like black boxes force users to switch attention from felicitous content to obstinate format.

On top of the opacity inadvertently designed into software systems, IT use in real organizations depends on a great deal of social scaffolding which is largely invisible in SOP manuals, engineering diagrams, and management *PowerPoint* slides. Scott observes that abstractions which make different entities commensurable and thus controllable leave out local idiosyncrasies which turn out to be critically important to the functioning of society: "These state simplifications...like abridged maps...did not successfully represent the actual activity of the society they depicted...they represented only that slice of it that interested the official observer...[and] when allied with state power, would allow much of the reality they depicted to be remade."[102] Explicit data processing on connectivity charts or standard operating picture is just the tip of the iceberg of actual information processing.[103] Ciborra notes "the importance of the unfinished, the untidy, the irregular, and the hack as fundamental systems practices" and observes that in corporations, "Ethnographic research about the implementation and use of information technology suggests that quite often even in large organizations: leadership is missing; and the technology is drifting, as if out of control."[104] So too in the belly of military command and control, systems are a chaotic mess of incompatible standards, inefficient data structures, Rube Goldberg expedients, and frustrated officers who have to deal with the mess.

With high information friction, the center is unsure of what to measure and how to measure it. Decision-making becomes confused and delayed, or else myopic and neurotically accelerated toward behavior which is locally counter-productive. The shadow of the world cast

---

[102] Scott, *Seeing Like a State,* p. 3

[103] John Seely-Brown and Paul Duguid, *The Social Life of Information* (Boston, MA: Harvard Business School Press, 2000); Greg Downey, "Virtual Webs, Physical Technologies, and Hidden Workers: The Spaces of Labor in Information Internetworks," *Technology and Culture* vol. 42, no. 2 (2001): 209-235; Heinrich Joachim Schwarz, "Techno-Territories: The Spatial, Technological and Social Reorganization of Office Work," Ph.D. Dissertation, Massachusetts Institute of Technology, Program in Science, Technology and Society (2003)

[104] Ciborra, *Labyrinths of Information*, 3, 21

on the cave of the "closed world" is only a filtered image of things that the organization is prepared to act on.

3.3.4.3 Political Mobilization

Abstractions not only leak, they are subject to deliberate politicization. Representations may be constructed for rhetorical purposes to persuade, distract, or mislead. Harvey Sapolsky describes how the Navy Special Projects Office created a multi-media management center showcasing Program Evaluation & Review Technique (PERT) for the Polaris ballistic program. Flashy computerized graphics created an aura of efficiency and diverted critical attention from unconventional management practices. One participant recalled that PERT "had lots of pizzazz and that's valuable in selling a program...The real thing to be done was to build a fence to keep the rest of the Navy off us. We discovered that PERT charts and the rest of the gibberish could do this. It showed them we were top managers."[105] Centers of calculation may serve a rhetorical purpose to demonstrate an air of mastery, rather than the functional work of actually achieving it.

An important theme in the sociology of scientific knowledge is that a lot of rhetorical effort goes into the establishment of the authority of scientific claims. For a claim to be "scientific" it must be seen by scientists and policy-makers as objective, significant, and apolitical; ironically, it takes a great deal of political effort to create and maintain these boundaries.[106] Because each scientific or intelligence representation summarizes an entire network of interactions behind it, challengers who dispute the claim have to challenge this network and expose the flaws in its construction. They try to produce stronger networks to produce counterattacking inscriptions that "force dissenters into believing new facts and behaving in new ways."[107] Latour describes how impressive-looking graphics produced by strong networks give "unique advantage...in the rhetorical or polemical situation. 'You doubt what I say? I'll show you.' And, without moving more than a few inches, I unfold in front of

---

[105] Harvey M. Sapolsky, *The Polaris System Development: Bureaucratic and Programmatic Success in Government* (Cambridge, MA: Harvard University Press, 1972), 124

[106] Sheila Jasanoff, "Contested Boundaries in Policy-Relevant Science," *Social Studies of Science* vol. 17, no. 2 (1987): 195-230

[107] Latour, "Drawing Things Together," 25. Doing so is not just a matter of reasoned argument. Stronger networks mobilize credentials, like-minded colleagues, grants, the construction of confounding experiments, and finally, publication of persuasive summaries and distilled representations of this effort in authoritative, legitimate venues.

your eyes figures, diagrams, plates, texts, silhouettes, and then and there present things that are far away and with which some sort of two-way connection has now been established."[108]

The politics of knowledge evaluation in high-stakes security arenas is particularly contentious. Controversies surrounding the evaluation of intelligence on Iraqi weapons of mass destruction prior to the 2003 invasion,[109] the relative merits of MX versus Trident II nuclear missiles,[110] or discrepant Vietnam order of battle assessments by the Defense Department and the CIA,[111] all made for quite dramatic and public quarrels. Because parties aggressively deconstruct knowledge claims in order to undermine the authority of their rivals, "ground truth" in such controversies can be elusive to ascertain in the midst of the spat. Quantified statistics of conflict casualties, refugee flows, illicit trafficking, and militant force levels are particularly vulnerable to politicization because they provide an air of scientific authority for estimates which are often unreliable due to the self-hiding nature of illegal phenomena.[112] As just one example, reputable Western media outlets repeated invented numbers and graphic fabrications about Israeli atrocities in April 2002: "The 'Jenin massacre' has become a damaging social fact, even though it never occurred."[113] Martin Van Creveld argues that many "information pathologies" in the U.S. Army in Vietnam stemmed an overreliance on quantified metrics: "Designed to produce accuracy and certainty, the pressure exercised from the top for more and more quantitative information ended up by producing inaccuracy and uncertainty."[114]

Military and intelligence centers of calculation are protected by classification boundaries. Secrecy, which Weber describes as the fighting posture of bureaucracy, obfuscates knowledge assessment by protecting actors from attack by political rivals and enhancing rhetorical authority through appeal to official secrets.[115] Intelligence agencies become attractive targets for

---

[108] *Ibid.*, 36

[109] Robert Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca NY: Cornell University Press, 2010)

[110] Graham Spinardi, *From Polaris to Trident: The Development of U.S. Fleet Ballistic Missile Technology* (Cambridge University Press, 1994)

[111] Sam Adams, *War of Numbers: An Intelligence Memoir* (Steerforth Press, 1998)

[112] Peter Andreas and Kelly M. Greenhill, ed., *Sex, Drugs, and Body Counts: The Politics of Numbers in Global Crime and Conflict* (Ithaca NY: Cornell University Press, 2010)

[113] Kelly M. Greenhill, "Counting the Cost: The Politics of Numbers in Armed Conflict," in *Sex, Drugs, and Body Count,* ed. Andreas and Greenhill, 148

[114] Martin Van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985), 259

[115] Max Weber, *From Max Weber: Essays in Sociology* (New York, NY: Oxford University Press, 1946), 233

politicization in high-profile controversies because they enjoy monopoly position as the government's keeper of secrets, which enhances the purely rhetorical value of intelligence. At the same time secrecy undermines elected official's interest in checking metastasizing bureaucracy or promoting more objective analysis because voters don't reward their attention to the organs of intrigue. Secrecy provides government agencies with cover to enrich organizational control, wealth, and autonomy at the expense of principals' interests.[116]

When centers of calculation are mobilized into politically-invested advocacy roles rather than reliable representation and rational control of the mission, information friction increases. Table 3-6 sums up the manifestations of information friction in the integration phase of the control cycle.

Table 3-6: Information Friction in Integration

	Low Information Friction	High Information Friction
• Centers of calculation	Panoptic "common operational picture"	Illegible/fragmented or insular/oblivious
• Abstractions	Dependable "black boxes"	"Leaky" implementation
• Decision-making	Efficient	Sclerotic or neurotic
• Mobilization of representations	Mission functional	Political rhetorical

3.3.5 Articulation

Articulation translates the representations in centers into action on the battlefield. It is perception in reverse. Recall that perception transforms the state of the world into symbolic records though constrained mappings from one media to another, across machine, human, and paper boundaries. Thus articulation—the word evokes a jointed apparatus and precision of speech—progressively transforms disembodied symbols into increasingly particular local situations. The discussions above about cascades of inscription, referential integrity and provenance all apply. Additionally, articulation highlights the problems of reconnecting with the world in order to change it and to improve control.

---

[116] Joshua R. Rovner, *Fixing the Facts: National Security and the Politics of Intelligence* (Ithaca NY: Cornell University Press, Forthcoming); Peter Galison, "Removing Knowledge," *Critical Inquiry* vol. 31 (Autumn 2004): 229-243; Joseph E. Stiglitz, "The Private Uses of Public Interests: Incentives and Institutions," *Journal of Economic Perspectives* vol. 12, no. 2 (1998): 3-22; Daniel P. Moynihan, *Secrecy: The American Experience* (New Haven, CT: Yale University Press, 1988); Zegart, *Flawed by Design*

3.3.5.1 Dead Reckoning

The integration phase disconnects symbols from the world of concern so that centers of calculation can combine perceptual cascades with representations in memory. Articulation must arrange a *future* reconnection with the world, so the problem of time is salient. Personnel have to compensate for the fact that their plots are constructed in a relation to a past state of the world, or at best an estimate of its current state. *Dead reckoning* extends the plot of past activity out in a constrained manner to estimate the future position of the same activity, based on a model of how it should evolve in the mean time. The estimate relies on internal constraints like timestamps on data as well as models of external constraints, as in the relationship between rate, time and distance or the growth of an insurgent population with new recruits. The estimate may simply be "no change," especially for fixed targets like buildings which are assumed not to move (although their function can change). In any real navigation or intelligence tracking problem, there is regular feedback to correct dead reckoning with records of updated observations. This positing of feedback simply assumes that the reconnection has already occurred, since even perceptual sensing is a form of physical contact. Between contacts, dead reckoning or inertial navigation is the only option.

When information friction is low, then estimates derived through dead reckoning will place personnel in the world in such a way that they aren't terribly surprised by what they find. The validity of estimates depends on their ability to enable (or prevent) desired (or feared) reconnections without surprising breakdowns. Surprises would include unexpected collisions, as in fratricide or collateral damage, or an inability to intercept an enemy, as in a "dry hole" during a raid where the target has fled or was never present.

3.3.5.2 Contact

The process of military articulation ultimately culminates on the battlefield. The effect of successive material transformations is to orient combatants on the battlefield, but it is up to them to close the loop. Radar controllers can place interceptors in the way of enemy fighters, and commanders can place soldiers at the door of an insurgent's house, but it is up to them to make the kill. There is more information inherently in the structure of the ensuing action than can ever be predicted or recorded. The close fight is the ultimate black box.

In classic military usage, "fixing" an enemy meant holding his forces in contact, exchanging fire and casualties and preventing retreat. While finding the enemy was an epistemic problem addressed with scouts and spies, fixing involved hard fighting en route to "finishing," or rendering the enemy combat ineffective through rout, surrender, or annihilation. The fix phase in modern information-intensive targeting is more a matter of tracking a target. Actual fighting is often confined to a burst of surgical violence. If you once had to fight the enemy in order to know him, now it seems you have to know him to fight. In the same vein, the boast is often made of U.S. smart weapons that "anything we can find we can hit, and anything we can hit we can kill." While this turns fixing into an epistemic problem, the concept of *maintaining contact* with the enemy remains germane. Tracking, like fighting, involves keeping the enemy in material contact, but with sensors rather than soldiers. The close collection, like the close fight, must remain shrouded in its particular mystery.

3.3.5.3 Feedback

Perception begins and articulation ends in material contact. Control cycles are continuous, as captured in the practical military notion of the intelligence-operations cycle. Every patrol is an opportunity to gather data and to affect the battlefield. Every firefight is a chance to learn something about the enemy. Mission debriefs, patrol reports, shooter statements, and guncamera video are all representations in perceptual cascades that begin in an articulation.

Iterated cycles of feedback gradually improve the coordination between the representations in centers of calculation and the structure of the operating environment.[117] Brian Cantwell Smith likens any mental act of knowing to an acrobat trying to keep a flashlight focused on another acrobat as they both jump around; any cognitive system has "to connect in such a way as to support appropriate (coordinated) disconnection, and to disconnect in such a way as to support appropriately prior or subsequent connection."[118] Likewise a military organization must constantly arrange for and compensate for contact and disconnection.

The repeated, frequent physical interactions between the friendly and enemy structures via cascades of inscription bring these different structures into closer and closer coordination. Closer coordination progressively lowers the uncertainty of each reconnection. Finally it

[117] This is a more tactical and representationally-focused version of "cybernetic learning" described by Steinbruner, *Cybernetic Theory of Decision*

[118] Brian Cantwell Smith, *On the Origin of Objects* (Cambridge, MA: MIT Press, 1996), 298

becomes possible to launch an assault on a target. These series of mutually-enabling connections and disconnections between hunter and prey coordinate the construction of the hunter's internal representations with the evolving structure of the battlefield. This feedback-driven coordination is a far cry from simply mirroring an independent reality.

3.3.5.4 Dead Space

A tactically maneuvering soldier seeks *dead space* to protect himself from enemy eyes and bullets. In distributed cognition, the target's problem is to find or create cover and concealment where the hunter's collection can't reach. The enemy's operational security or secrecy is one way of creating dead space in order to maintain and preserve the material basis of his information and action from corrosion and compromise. The enemy can also disrupt counterinsurgent intelligence through direct attack on collection sources and communication systems, or cooptation of intelligence sources to deceive or infiltrate the counterinsurgent. The hunter can also inadvertently create dead space for the target. High information friction in the counterinsurgent organization impairs the establishment, communication, or correlation of perceptual cascades, thus disabling effective articulation. The behavior of the enemy is constrained by real structure in the world, but any misunderstanding of this structure makes it hard for the counterinsurgent to engineer the intersection of articulation cascades with the target. Such problems will be described in depth in the next chapter on the causes of information friction and in the ethnographic chapters.

The blindness of centers of calculation creates dead space. Scott's *Seeing like a State* criticizes the destruction of local knowledge through the standardizing lens of bureaucratic power. Yet his other books highlight the ability of peasants to resist cooptation by living in the state's dead space.[119] If state power depends on the ability to make a population legible, then by the same token, Scott argues, resistance is also based on the ability to work around this legibility, by leveraging resources that are not circumscribed by official measurement. Likewise, intelligence operations unfold and insurgents plan their attacks while striving to remain illegible in the dead space of their adversary's counterintelligence efforts. There is a contested zone between any adversarial actors across which standardized epistemes cannot penetrate.

---

[119] James C. Scott, *Weapons of the Weak: Everyday Forms of Peasant Resistance* (New Haven: Yale University Press, 1987); James C. Scott, *The Art of Not Being Governed: An Anarchist History of Upland Southeast Asia* (New Haven, CT: Yale University Press, 2009)

Table 3-7 summarizes the manifestations of information friction in the articulation phase of the control cycle, including the considerations shared with the perception phase (indicators shared with Perception appear in italics).

Table 3-7: Information Friction in Articulation

	Low Information Friction	High Information Friction
• *Cascades of inscription*	*Constrained transformations*	*Corrupted, noisy, equivocal*
• *Referential integrity*	*Preserved*	*Broken*
• *Provenance*	*Recorded & reliable*	*Adverse selection & veracity bubbles*
• Dead reckoning to contact	Reliable reconnection	Unpredictable collision or unable to connect
• Feedback	Triangulation and self-correction	Allow enemy "dead space"

3.3.6 Closing the Loop

To sum up this discussion of distributed cognition, people and machines share the computational burden of constructing representations of the world by implementing loops within loops of perception, integration, and articulation. IT constrains and enables people to perform routines and subroutines, exploit standardized abstractions, combine information into panoptic pictures, and make error-correcting adjustments through feedback. The constrained propagation of representations across radio waves, mechanical instruments, computer files, map plots, and human minds preserves referential integrity of representations to their original provenance on the battlefield. The entire sociotechnical information system arranges cascades of inscription to and from disconnected centers of calculation which coordinate reliable reconnection with stabilized features of the environment. Control loops thereby close on the entities in the world the organization cares about controlling, whether allies or enemies. The closure of control loops on the objects of concern enables the organization to measure and reduce the gaps between its goals and the state of the world.

At least that's what happens when information friction is low. This happy state of affairs can also be called *enterprise integration*, the technocratic ideal of command and control system builders and RMA doctrine writers. However, reality usually diverges. At each stage in the discussion I have highlighted ways in which high information friction entails the breakdown, confusion and politicization of information processes. The net effect of these corruptions is to prevent control loops from closing on the right things in a timely manner. This may be because

processes are literally broken and the system "goes stupid" on some ballistic trajectory, because there is controversy over what the "right things" actually are, or because the system is politically captured by parochial interests and refocused on counterproductive ends.

Logically, control loops have two different failure modes. I have been lumping both together as high information friction because they often occur together at different levels of analysis; logically, however, it's possible to distinguish two different kinds of high information friction. The loop can fail to close altogether, or it can close prematurely on the wrong things. *Interference* suffers from uncoordinated internal control, while *insulation* suffers from too much internal control. With high information friction, the computational problem can be either unsolved or oversolved. Either way, the control loop fails to close on objects of concern and creates dead space. As everywhere with multilevel control systems, insulation at one level or for one group might be experienced as interference at another. These two unhappy states of affairs are so bound up with the problem of institutional consensus, one of the major causes of information friction, that I will leave further discussion of them for the next chapter.

3.4 Summary of Empirical Manifestations

Information friction is an abstract theoretical notion that aggregates different measures of the health of organizational information processing, which I have harvested from sociology of technology and cognitive science literatures. This notion provides a net qualitative measure of how hard or easy it is for a distributed cognitive system to make sense of the world. When information friction is low, then stable networks enable personnel to share information and improve their "situational awareness," which in turn improves operational control of the battlefield in line with RMA expectations. When information friction is high, however, then systems are dysfunctional, unpredictable, and politicized. Control cycles don't work as intended, organizations can't agree on what their intentions are, and politicized manipulation of technical protocols degrades performance. Although military organizations are flush with IT designed to reduce uncertainty, command and control nevertheless stumbles around in the "fog of war."

Table 3-8 consolidates the empirical indicators of information friction. Not all indicators necessarily have to be correlated, and some might even work against each other in some situations. Information friction is a net assessment of these factors, which in their overall

tendency to be low or high, contribute to the performance or dysfunction of command and control.

Table 3-8: Empirical Manifestations of Information Friction (IF)

		Low Information Friction	High Information Friction
Phenomenology *(qualitative experience of participants in the information system)*			
IF1.	Sense-making	"Situational awareness"	"Fog of war"
IF2.	Attention	{actor → tools} → world	actor → {tools → world}
IF3.	Format	Transparent usage	Obtrusive breakdown
IF4.	Content	Felicitous/available	Unreliable/unavailable
IF5.	Uncertainty	"Aleatory" values on variables	"Epistemic" models & methods
IF6.	Politicization	Harmony	Controversy
Cognitive Prosthetics *(IT usage amplifies human perception or misperception)*			
IF7.	Affordance	Suggest appropriate action	Mask possible action
IF8.	Perceptual Offload	Reduce cognitive load	Uncritical acceptance
IF9.	Precomputation	Spread load over time & people	Hidden assumptions
IF10.	Precision/Complexity	Sophisticated measurements	Dependency & opacity
Distributed Cognition *(Systemic qualities of human-machines implementation of control cycles)*			
IF11.	Computational Goals	Defined/shared	Ambiguous/controversial
IF12.	Implementation	Efficient	Ends-means misalignment
IF13.	Routine Performance	Heedful interrelating	Mindless execution
IF14.	Command and Control Doctrine	Orients practitioners to bureaucratic format	Simplistic omission of messy realities
Perception *(Transduction of environmental situations into detached symbols)*			
IF15.	Cascades of inscription	Constrained transformation	Corrupted, noisy
IF16.	Referential integrity	Preserved	Equivocal
IF17.	Provenance	Recorded & reliable	Unknown
Integration *(Combines incoming information with information in memory)*			
IF18.	Centers of calculation	Panoptic "common operational picture"	Illegible/fragmented or insular/oblivious
IF19.	Abstractions	Dependable "black boxes"	"Leaky" implementation
IF20.	Decision-making	Efficient	Sclerotic or neurotic
IF21.	Mobilization	Mission functional	Political rhetorical
Articulation *(Transduction of symbols into action in the environment)*			
IF22.	Dead reckoning to contact	Reliable reconnection	Unpredictable collision or unable to connect
IF23.	Feedback	Triangulation & self-correction	Allow enemy "dead space"
IF24.	Closure	Close on entities of concern (enterprise integration)	Hung open or premature closure (interference and insulation)

My goal has been to explicitly identify factors from the sociology of technology and cognitive science literatures which are too often overlooked in debates over IT and military performance and technocratic treatments of command and control and intelligence. There

remain many important questions about the correlation of, endogenous causation between, and nonlinear interactions among these many different components, but I leave these open as beyond the scope of my dissertation.

3.5 The Effects Information Friction on Military Performance

This section will connect distributed cognition to military performance in war. In the foregoing discussion I have offered some examples of how manifestations of low or high information friction cause military outcomes. This section explicitly states causal relationships (Figure 3-7). My intent is to show the specific ways in which distributed cognition and information friction matter for the military outcomes that analysts and policymakers care about.

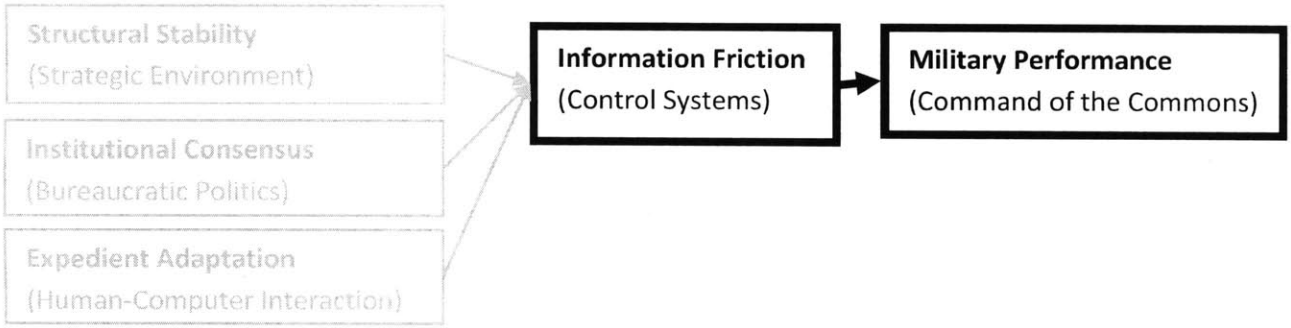


Figure 3-7: Causal relation of information friction to military performance

3.5.1 Command of the Commons

The post-Cold War era has been distinguished by an unmatched preponderance of U.S. military power: the system is structurally unipolar. Barry Posen argues that U.S. hegemony is founded on its military mastery of ungoverned spaces at sea, in the air, and outer space, or "command of the commons." Allies and potential adversaries more or less agree on the relative distribution of power there: the U.S. is preponderant. Only in contested zones on the ground (up to the 15,000 ft. ceiling of most man-portable air defense systems) can adversaries offer serious military challenge. Posen lays out both the foundations and limitations of U.S. power in hopes of inspiring policies of strategic restraint consistent with the intractable problems of contested zones.[120]

---

[120] Barry R. Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security* vol. 28, no. 1 (2003): 5-46. Ironically, given Posen's intention to encourage restraint of U.S. power, the U.S. military appears to have embraced his concept as a normative objective to consolidate it. For example, Chairman of the Joint Chiefs of Staff, *Capstone Concept for Joint Operations* (Washington, DC: Department of Defense, 15 January

To generalize Posen's framework, the zone of command is a well-ordered hierarchy, while the contested zone is a chaotic anarchy. The offense seeks to expand its zone of command into the contested zone. The defense seeks to resist and to expand the contested zone into the offensive zone of command, while maintaining and expanding the defensive zone of command. Organizations in the contested zone are not able to establish command over their opponent, and they have difficulty controlling themselves because of active disruption of their infrastructure and operations. In the course of war, organizational structure and processes are simultaneously built out and torn down in the turbulent borderland between these two extremes.[121] Low information friction promotes achievement of command of the commons. High information friction expands the contested zone.

One striking feature of Posen's domains where the U.S. enjoys primacy—air, sea, and space—is that they all involve heavy use of networks that tend to provide the sorts of benefits that RMA theory expects. Stable satellite communications link units in the field to neighboring units, higher headquarters, and "reach-back" organizations in the U.S. that provide intelligence and planning products. The Global Positioning System (GPS) guides precision munitions and enables friendly forces to coordinate maneuvers and avoid fratricide. A formal collection-management bureaucracy delivers intelligence products through reliable channels to tactical units. The U.S. Navy controls the world's oceans with fewer than 300 ships, thanks in large part to robust subsurface acoustic networks (SOSUS), airborne maritime patrol, satellite monitoring

---

2009), 3, states that "maintaining sufficient control of the global 'commons' -- areas of sea, air, space, and cyberspace that belong to no one state -- thus will remain a vital imperative of future joint force design"; similarly, on the official 2010 Quadrennial Defense Review website, see Under Secretary of Defense for Policy Michèle Flournoy and Shawn Brimley, "The Contested Commons," http://www.defense.gov/home/features/2009/0509_qdr/flournoy-article.html. The addition of "cyberspace" as a global commons is notable in these official documents, although it raises the question whether cyberspace is really a domain like air, sea, and space. As a normative doctrine, the whole "commons" discourse raises the question of whether the U.S. is acting in the "common good" or simply securing military control of "common" ungoverned space. This is just a new twist on the old security dilemma: is U.S. power supplying a public or private good? The use of the euphemistic term "access denial," for China's acquisition of defensive capability to counter U.S. power projection, flows naturally from this "commons" doublespeak: China sees U.S. command as a private good while the U.S. represents its control as being in the public interest.

[121] This regime is sometimes called "the edge of chaos" in the literature on complexity. It is an area where the emergence of evolutionary novelty is maximized. The next chapter will discuss how information friction can be an engine for innovation and an endogenous cause of itself. On "the edge of chaos" see Stuart A. Kauffman, *The Origins of Order: Self-Organization and Selection in Evolution* (New York, NY: Oxford University Press, 1993); John Henry Holland, *Emergence: From Chaos to Order* (Reading, MA: Addison-Wesley, 1998); James Gleick, *Chaos: Making a New Science* (New York, NY: Penguin, 1987)

of maritime electronic emissions, and global infrastructure for intelligence fusion.[122] The ships, aircraft, and submarines of a carrier strike group, as well as neutral or suspicious contacts, although separated by hundreds of miles, are tracked on three dimensional plots shared throughout the group. In the air, ground and airborne early warning systems track and classify air targets and vector advanced interceptors. By and large in these areas, target identification and tracking is reliable, and networks enable far-flung forces to communicate and self-organize against threats.

The external stability of the sea and aerospace domains—discussed in the next chapter—contributes greatly to the low information friction which promotes command of the commons. Friction is also lowered by internal consensus, also discussed in the next chapter. As a result the services reach stable agreement about "lanes in the road" regarding who has responsibility for which missions, who produces and validates different kinds of information, and how this information will be shared via what protocols. Weapons procurement can be carefully managed with long lead times in the expectation that today's missions will still be important tomorrow. The services can develop realistic training evolutions and professional training pipelines to exercise their capabilities. The enabling infrastructure in the zone of command is stable, reliable, and predictable (the Weberian ideal of formal bureaucracy), and it is protected by geographical and military boundaries from the interfering reach of adversaries.

By contrast, information systems don't work so well in Posen's contested zones. Physical circuits cannot be established because the enemy or the environment cuts, jams, or interdicts them, or it is impossible to establish them in the first place (because transmitters can't be erected or powered or cable can't be laid in). Logical communication and encryption protocols are uncoordinated and incompatible, frustrating interactions between units and delaying or garbling requests for fire or reinforcement. Databases are confronted with new types of entities and situations that they aren't designed to track. All forms of Clausewitzian friction (danger, exhaustion, uncertainty, entropy, political chafing) increase in the contested zone. Knowledge does not float freely, but is produced and coordinated through material networks subject to breakdown, whether as a result of external instability or internal disensus, both

---

[122] Ford and Rosenberg, *The Admirals' Advantage*; Norman Friedman, *Seapower and Space: From the Dawn of the Missile Age to Net-Centric Warfare* (Annapolis, MD: Naval Institute Press, 2000)

discussed in the next chapter. High information friction exacerbates contestation and degrades command of the commons.

3.5.2 Targeting

Targeting is the heart and soul of network-centric warfare. The targeting cycle is a control loop, and with low information friction it is implemented efficiently. Targeting guidance is aligned with political objectives for the campaign. Intelligence services identify the target systems that are most appropriate for the stated commander's objectives. Representations of targets accurately represent their real location, function, and identity. The weapons that are paired against them are able to achieve the desired effects. Target systems are attacked systematically, achieving "shock and awe" to paralyze the enemy's ability to understand and react to what is happening. The "kill chain" is able to find, fix, track, target, engage, and assess fleeting mobile targets with alacrity. Risks of collateral damage are minimized through deliberate modeling of weapons effects with civilian casualty estimates.

With high information friction, targeting becomes imprecise or even counterproductive. There is controversy over targeting objectives. Intelligence misidentifies targets and fails to identify important ones. The force attacks target systems sporadically and incoherently, leaving the enemy time to reconstitute and repair damages. Noisy or uncoordinated targeting processes cause collateral damage with unpredictable second-order effects (*e.g.*, badly mistaken identity as in the Chinese Embassy in Belgrade, or embarrassing media events like accidental wedding party bombings or attacks on reporters), as well as tragic fratricides. In conditions of bureaucratic insulation, targeting is displaced: the targeting cycle runs on and on like an automaton after whatever "low hanging fruit" appears, while the enemy's important centers of gravity remain unmolested. Targeting becomes captured by parochial organizational interests, and secrecy protects them from audit. Dead space abounds for the enemy, who enjoys freedom to frustrate targeting plans.

3.5.3 Operational Style and Coordination

A military with low information friction has high "situational awareness" of the position and disposition of its own forces and enemy forces. This "information dominance" allows friendly forces to take up favorable tactical positions to get the jump on the enemy. "Dominant maneuver" by ground forces envelops enemies who are unable to respond and either forces them

to surrender or handily annihilates them. Information-intensive war is a war of maneuver. By substituting information for mass, fewer friendly forces have to be committed, because they are cued to show up in the right place at the right time, and they can dispatch their adversaries safely from long distances. "Reachback" organizations a continent away provide up-to-date intelligence and operational planning support in order to further reduce the forward footprint. Every platform is a "sensor" networked to other "shooters," and with robust communications they are able to "self-synchronize" their combined-arms force to overwhelm the hapless enemy.

Under conditions of high information friction, by contrast, the organization has trouble finding, fixing, and finishing the enemy. Combat grinds down into a costly protracted contest of attrition. The enemy has to be found by running into him or awaiting an ambush. Uncertainty about the location and activity of the enemy compels the military to dip into its reserves in order to compensate for wastage and to flood the battlefield with troops in hopes of improving the statistical odds of stumbling upon the enemy. They substitute mass for the lack of information. Headquarters becomes a frenzied circus as staff officers fret over their lack of control and get pulled into petty internecine spats. Commanders micromanage their forces and impose further inefficiencies on organizations already struggling to deal with a frustrating enemy.

3.5.4 Conflict Duration and Casualties

The point of achieving "information dominance" in RMA doctrine is to speed up decision cycles, to "turn inside the enemy's OODA loop," in order to go for the jugular and bring the conflict to a timely close. Low information friction enables commanders to make quicker and better decisions, and to strike the enemy's "critical nodes" before he strikes back. Because the information system is able to reliably and repeatedly close on the enemy's forces and enabling command and logistics networks, knocking them out with precision weapons that keep collateral damage to a minimum, the enemy will not be able to stay in the fight for long. A shorter war also means fewer casualties. Furthermore, since forces are able to substitute information for mass through long range precision strikes and agile maneuvers, fewer people will be exposed to enemy fire, and those who are will be able to more quickly achieve tactical advantage.

High information friction lengthens the conflict and kills more people. Militaries can't find the right things to kill, and they kill the wrong things; therefore, they have to hang around longer to finish the job they started, and they have to clean up the messes they've created in the

process. The contest of attrition drags on as the targeting system flails about looking for something available to hit. Decision-making becomes delayed and unfocused, or neurotically hyperactive against whatever happens to demand attention. Commanders in the field and politicians back home begin to argue about objectives and timelines. The enemy perceives this dithering as a weakening of the will to fight, and so resolves to hang on even longer. The enemy concludes, correctly, that the occupying force is confused, tired, and eager to get out of a controversial and costly war.

3.5.5 Outcome

Low information friction enables decisive victory. After the rapid rout, both adversaries, as well as third party observers, have reliably measured the balance of power. The settlement is widely perceived as legitimate, so war is unlikely to threaten again in the near future. High information friction, by contrast, makes victory uncertain or ambiguous at best. Even if the enemy capitulates or fades away after a long protracted bruising, the anticlimactic dénouement lacks any meaningful catharsis. The issues that started the war either remain unresolved, or the issues that arose during its course have sown the seeds of recidivism in the near future. The settlement lacks popular legitimacy.

3.5.6 Relative Information Friction

Low information friction enables victory, but this does not mean the high friction necessarily denies it. The enemy might be even worse off. In war it is ultimately not absolute but relative power that matters. Both sides might suffer from tremendous information friction, with both making mistakes that contribute to the protraction of the conflict. The balance of friction is an important consideration, although I do not have the space to develop it here.[123]

3.5.7 Information Friction is Everywhere but not Everything

A military needs IT, but it obviously needs ships, airplanes, tanks, troops, bases and a defense industry as well. The information system enables the management of complexity, but the military must still have something to manage. Moreover, those weapons and the human capital to use them must be up to the measure of their adversaries. Weapons procurement, grand

[123] The idea of relative friction is discussed by Barry D. Watts, "Clausewitzian Friction and Future War, Revised Ed." National Defense University McNair Paper, no. 68 (2004)

strategy, personnel policy, and civil military relations all contribute to military power.[124] Information systems are necessary but far from sufficient for victory. Therefore, information friction is not an independent determinant for victory. It is well beyond my scope here to distinguish the relative contribution of all these factors to military power. They were listed in Figure 3-1 just to note their importance outside of command and control. It also helps to be lucky.

That said, I have defined information friction as the aggregation of other influences on organizational command and control and the penultimate factor shaping performance. Other factors shape the pieces that contribute to command and control and the forces which are controlled, but information friction describes the organization's ability to use any of it in clearheaded or muddled way. When it comes time for a military to make "cash payment" in battle, as Clausewitz put it, it will have to grind through information friction to do so. Information friction should properly be thought of as a conditioning influence on all the other determinants of military effectiveness. It's a sort of drag that introduces unpredictable perturbations into the way the rest of the system comes together.

3.5.8 Summary of Hypotheses

This chapter has described *information friction* as the political and technical struggle to coordinate representational protocols with the world of operational concern. It is a theoretical notion which gathers together the complexities of human-computer interaction that cause actual information systems to diverge from technocratic ideals. Any of the manifestations of friction (Table 3-8 above) might cause any of the particular battlefield effects just reviewed and summarized in Table 3-9. Desirable military effects on the left side of Table 3-9 are those which RMA enthusiasts expect to follow from IT networks and the "right" Joint doctrine. The undesirable effects on the right, curiously enough, tend to occur in actual wars.

---

[124] *Ibid.*; Allan R. Millett, Williamson Murray and Kenneth H. Watman, "The Effectiveness of Military Organizations," *International Security* vol. 11, no. 1 (1986): 37-71; Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton University Press, 2004); Martin Van Creveld, *Fighting Power: German and U.S. Army Performance, 1939-1945* (Greenwood Press, 1982); Allan R. Millett and Williamson Murray, *Military Effectiveness: The First World War* (New York: Routledge, 1991)

Table 3-9: The Effects of Information Friction on Military Performance (IF→MP)

Military Performance	Low Information Friction ↓	High Information Friction ↓
MP1. Military Power	"Command of the Commons"	"Contested Zone"
MP2. Targeting	Precise, systematic, effects-based	Haphazard, displacement
MP3. Targeting Error	Controlled/minimized, accurate estimates of collateral damage risk	Unexpected intensity/amount of collateral damage & fratricide
MP4. Operational style	Maneuver	Attrition
MP5. Mass	Substitute information for mass	Consumption of reserves & slack
MP6. Coordination	Self-synchronizing	Incoherent or micromanaged
MP7. Conflict duration	Rapid tempo	Protracted
MP8. Casualties	Low	Bloody, costly
MP9. Outcome	Decisive	Ambiguous
MP10. Popular perception	Legitimate	Controversial

These are general probabilistic hypotheses. Information friction is a continuous, aggregative, ideal type variable which describes the general tendency of its components to vary one way or the other and, in the net, to cause variance in important operational effects which military analysts and policymakers care about. I leave open as beyond my scope many important questions about specific correlations and endogenous linkages. This thesis stops well short of analyzing correlations among particular effects. It also does not connect the detailed components of information friction (Table 3-8) to each specific outcome (Table 3-9), because there are a lot of tangled nonlinear relationships. Any specific case study of information friction must go into detail to trace just how information system breakdowns lead to unfortunate performance outcomes, and vice versa.

Effective distributed cognition can hardly be taken for granted. Intelligence, targeting, and command systems break. The reason that they ever work at all is that there's a lot of dark matter holding cyberspace together, so to speak. As there is more mass in the universe than astrophysicists measure directly, so there is more human scaffolding of networks than a technocratic focus on IT alone or a Cartesian view of knowledge can account for. Information is not virtual, weightless, or free-floating, but rather it is embodied in technology and work-processes which generate friction. The next chapter offers hypotheses on the causes of information friction.

Chapter 4: Causes of Information Friction

> "Among essentially technical factors, the specifically modern means of communication enter the picture as pacemakers of bureaucratization...The degree to which the means of communication have been developed is a condition of decisive importance for the possibility of bureaucratic administration."
> – Max Weber[1]

4.1 Defining the Causes

Political and technical control systems are deeply intertwined, and they can generate unintended consequences. The previous chapter introduced the notion of information friction, the persistence of Clausewitzian friction in the information age. Low information friction improves a military's situational awareness so that it can close control loops repeatedly and reliably on the enemy, which improves performance as per "revolution in military affairs" (RMA) expectations. Under high information friction, by contrast, the very technologies designed to reduce uncertainty become sources of breakdown, uncertainty, and politicization. Information system pathologies degrade military performance. Under what conditions should we expect high levels of friction? Information friction emerges in the everyday usage of information technology (IT), but its causes are not just technical. This chapter describes how the structure of the battlefield, bureaucratic competition for control of technical protocols, and local interactions with available IT all shape the viability of information systems. The increasing complexity of modern information systems and of military missions tends to exacerbate information friction, which requires an organizational capacity to work through it in war.

4.1.1 Three Levels of Analysis

Following Kenneth Waltz's classic *Man, the State, and War*, international relations theory customarily considers the causes of security phenomena in three levels of analysis.[2] "First image" theories treat the psychology, beliefs and behavior of individuals. "Second image" theories consider the domestic and bureaucratic characteristics of states. "Third image" theories treat the anarchic structure of the international system. I will generalize these a bit further than Waltz to describe the basic idea that individuals and machines work in hierarchically-structured organizations, which collectively interact in an anarchically-structured environment composed of

[1] Max Weber, *Essays in Sociology* (New York, NY: Oxford University Press, 1946), 213
[2] Kenneth N. Waltz, *Man, the State, and War* (New York, NY: Columbia University Press, 1954)

other hierarchical organizations. I will use these three levels of analysis—strategic structure, bureaucratic politics, and human computer interaction—to describe the causes of information friction.

I do not consider "technology" as a separate exogenous factor because it is so embedded in everything an organization does, and doing so leads to the sort of technological determinism that RMA proponents embrace and I am trying to avoid. Instead, I disaggregate aspects of technology across all three. Distributed cognition employs individual people and machines working at the first image. They collectively form bureaucratic systems that politically control technical protocols at the second. Their computational problem is oriented toward competition with adversaries and allies at the third. These levels are rough cuts at a lot of complexity, but they describe categories of causes which can be discriminated from one another and which encompass interestingly different influences on information systems; they "carve nature at its joints." I will not seek to determine the relative importance of causes at the different levels in this project, but rather the more preliminary task of specifying them.

A basic question about organizational perception is the relationship between third image objects of knowledge and second image means of knowing them. The classic problem in the philosophy of knowledge is the relationship between the objective world and subjective beliefs. Philosophers sometimes refer to their interdependence as "the hermeneutic circle" because the external world causes perception in the brain while cognitive models and social institutions structure interpretation of the world.[3] In distributed cognition, control loops traverse through contact with the battlefield to disconnected centers of calculation and back again. Cascades of inscription make definite material contact with the world, but participants in centers of calculation can only ever act on constructed versions of reality. They act on their interpretations to change the battlefield, and then perceive the result as feedback in a recursive cycle. Control loops are literally a hermeneutic circle, with one pole planted on the objective battlefield and the other in subjective centers.

---

[3] The concept goes at least back to the seventeenth century and Spinoza's observation that our understanding of nature is like our understanding of the Bible, where reading the details forms an understanding of the whole, but the whole influences our understanding of the parts. Its postmodern roots lie in Martin Heidegger, *Being and Time* (San Francisco, CA: Harper, 1962). See also Francisco J. Varela, Evan Thompson and Eleanor Rosch, *The Embodied Mind: Cognitive Science and Human Experience* (Cambridge, MA: MIT Press, 1991).

While flagging the interdependence between these two aspects of control, it's analytically useful to consider them separately. I use "structural stability" to describe the battlefield environment and "internal consensus" for the bureaucratic politics of information protocols. If structural factors are stable, then it makes sense to talk about the organization adapting to the problem or not. External stability provides scaffolding for building up reliable and repeatable routines in the information system. However, institutional dysfunction can adversely change the problem as enemies or allies react unpredictably. An overprovision of consensus could cause myopic insulation amidst an unstable battlefield. The distinction between external stability and internal consensus enables us to analyze any mismatch between them, which provides a basis for critiquing organizational policies and suggesting reforms.

A persistent wartime problem is the misalignment of "objective" structure and "subjective" institutions. Personnel at the first image might try to adapt their information systems to restore some alignment. Computer science distinguishes "design time" software development, which is when a programmer writes and compiles code into an executable binary file, from configurations that can be set and functions which bind only at "runtime." In any real system, however, the modular and layered architecture of modern IT provides many design options to runtime users via macros, scripts, database definitions, *PowerPoint* slide layouts, *etc.* Programmers use software while developing code, and users reconfigure their systems in order to manage data. Therefore, IT employment could be better characterized as "runtime design." Design time work in IT is often less about completing a finished program than providing a set of modular parts which humans and machines can mix and match for a tailored second-order design. I will use the term "expedient adaptation" to describe an organization's empowerment of personnel to adapt their information systems in order to relieve information friction.[4]

4.1.2 Scope Conditions for the RMA

These considerations across three levels of analysis suggest three conditions necessary for lowering information friction and thereby improving performance. They are necessary but not sufficient because factors like weapons, grand strategy, civil-military relations, and chance all affect military power. The first two conditions establish reliable control loops. The

[4] In previous drafts I just called this "runtime design," but I have found that term confuses more than it explains. Hopefully "expedient adaptation" more intuitively conveys the "runtime" part, although it lacks the connotation of well-constructed technology of "design."

information problem must be stable, firstly, which means that features of the world must be knowable in principle. Secondly, actors with a stake in the problem must reach a rough consensus about how to mobilize bureaucratic and technical resources to solve it. When both conditions are met, actors can coordinate "subjective" representations with the "objective" environment in order to thereby close control loops on the enemy. During wartime, however, it is inevitable that these two conditions will not be completely met. The enemy usually compromises external stability and bureaucratic pathologies undermine internal consensus. Personnel then have to struggle with a representational architecture that is uncoordinated with the structure of the world. The third condition, therefore, is that an organization must be able to relieve friction in real time. Specifically, it must lower barriers between technical expertise and operational needs in order to reconfigure sociotechnical systems on the fly. Expedient adaptation is the only emollient for information friction in wartime. It is not a panacea, however, because amateurism can generate negative externalities which increase friction.

Table 4-1: Information friction theory explains the causes and consequences of information friction

1. External Stability	Stable ontology, Technically possible connection, Cooperative enemy	Dirty battlefield, Unavailable connection, Frustrating enemy
2. Internal Consensus	Doctrinal agreement, Systems integration, Economies of scale	Political controversy, Fragmented protocols, Rent-seeking and myopic lock-in
3. Expedient Adaptation	Extensible technology, Technical expertise forward, User innovation support	Closed technology, Barriers to expertise, Rigid use/design boundaries
	↓	↓
Information Friction	"Situational Awareness," Enterprise integration & local initiative, Reliable content and efficient decisions Closure on the enemy	"Fog of War," Interference & insulation, Frustrating formats & methods Hung open or prematurely locked-in
	↓	↓
Military Performance	"Command of the Commons," Rapid, self-synchronizing maneuver, Systematic precision targeting, Decisive, legitimate outcome	"Contested Zone," Protracted, over-managed attrition, Targeting errors and displacement, Ambiguous, controversial outcome

Table 4-1 summarizes the theory. The previous chapter defined information friction and its consequences for performance (the bottom two rows). This chapter develops hypotheses about how factors at the three levels of analysis (the top three rows) cause information friction.

The historical emergence of sophisticated IT and complicated missions tends to weaken both external stability and internal consensus, which makes expedient adaptation all the more important.

4.2 External Stability on the Battlefield

The constraints of the physical world, the conventions of society, the technical state of the art, and the behavior of the enemy all shape the stability or instability of military information problems. Historically, of course, an organization has to learn about the nature of the problem as it experiments with solutions; a problem has to be stabil*ized*. It's analytically clearer, however, to consider the objective problem separately. In terms of the phases of distributed cognition, external stability concerns whether material connections in the perception and articulation cascades are even possible in principle. The integration of such possibilities is a matter that I will take up in the subsequent section on internal consensus.

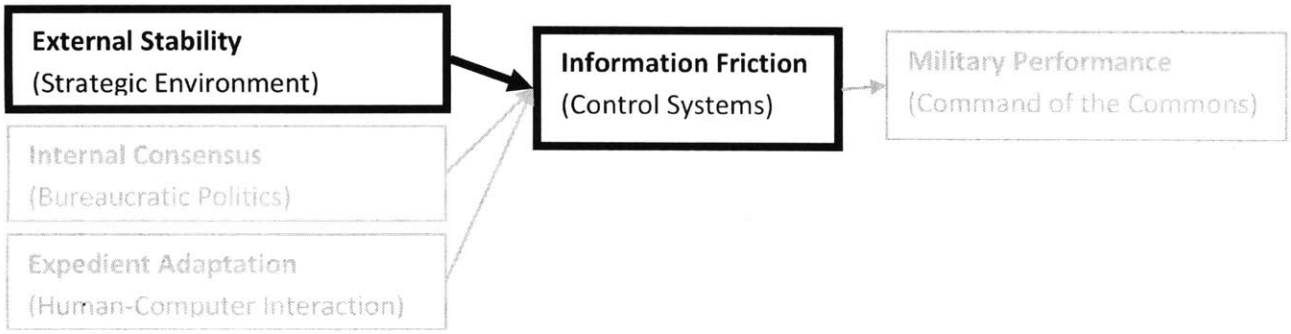


Figure 4-1: Causal relation between external stability and information friction

4.2.1 Battlefield Ontology

"Ontology" is a description of what types of things exist.[5] Battlefield ontology describes what sorts of entities a military cares about in its theater of operations. If the battlefield is clean and stable, then there's a better chance that assumptions built into models will be validated when they are cashed in during battle. Dirty battlefields have unstable ontologies, by contrast, so it's hard for combatants to find out which things matter and, moreover, those things are subject to change. Messy ontologies tend to generate more information friction.

---

[5] W.V.O. Quine, *Word and Object* (Cambridge, MA: The MIT Press, 1960), defines an ontology as any intensional account of what sort of things exist in a certain domain. This logical positivist concept is closest to the computer science usage of the term to define semantic types and relationships among them. Postmodernists sometimes use a more expansive connotation to treat the ultimate nature of reality or existence; I am not using the word that way here.

In computer science, an ontology is a semantic model of entities and relationships among entities in some practical domain. Thus a flight reservation system like *Travelocity* has to represent airlines, airports, flights, people, and tickets with various relationships between them: airlines schedule flights between airports; people buy tickets for flights; *etc.* The system's formal ontology tells other systems what it knows about, so that an application might thus book a trip by linking the flight database together with other databases of hotels and rental cars. A critical design assumption is that components of the data model map onto corresponding types of things in the real world. Models are true when they enable action without nasty surprises. Flight reservation systems work when passengers can show up at the airport and board an aircraft that goes where their ticket says it should. Overbooked flights, dropped reservations, and hijacked flights are all inconsistencies between the data model and the world. The system is similarly useless for planning a leg of the trip by boat or parachute because those options aren't in the ontology. The world that the system knows about is stable because airline companies, airport authorities, and the Federal Aviation Administration all have a stake in the maintenance of a stable world that can be modeled. Reservation systems model the things that are relevant for the proscribed and practical world of commercial airline ticketing. Stable patterns of structure and behavior allow system builders to take for granted the objective ontology of the world.[6] The notion of a perfect or exhaustive model of reality is incoherent because then the model and the world would be one and the same and thus impossible to manipulate and master in a detached center of calculation.[7]

---

[6] Some ontology writers get into scholastic debates about what sorts of things absolutely and exhaustively exist in the world, rather than optimizing their models for a particular domain of practice. This is a standard pragmatic critique of artificial intelligence, but the debate is regularly reenergized with every new domain-spanning abstraction to emerge from computer science. H. M. Collins, *Artificial Experts: Social Knowledge and Intelligent Machines* (Cambridge, MA: MIT Press, 1992); Hubert L. Dreyfus, *What Computers Still Can't Do: A Critique of Artificial Reason* (Cambridge, MA: MIT Press, 1992); Diana E. Forsythe, *Studying Those Who Study Us: An Anthropologist in the World of Artificial Intelligence* (Stanford, CA: Stanford University Press, 2001).

[7] Jorge Luis Borges takes the idea of perfect representation to its absurd logical conclusion in a one-paragraph story, "On Exactitude in Science," in *Collected Fictions*, Trans. Andrew Hurley (New York: Penguin, 1999):

> In that Empire, the Art of Cartography attained such Perfection that the map of a single Province occupied the entirety of a City, and the map of the Empire, the entirety of a Province. In time, those Unconscionable Maps no longer satisfied, and the Cartographers Guilds struck a Map of the Empire whose size was that of the Empire, and which coincided point for point with it. The following Generations, who were not so fond of the Study of Cartography as their Forebears had been, saw that that vast Map was Useless, and not without some Pitilessness was it, that they delivered it up to the Inclemencies of Sun and Winters. In the Deserts of the West, still today, there are Tattered Ruins

4.2.1.1 Types

If friendly and enemy forces are sorted into a standardized order of battle, then a finite set of symbols can represent the different types of vehicles and units that show up on the battlefield. New types that emerge in the midst of conflict, or modifications of existing types, complicate categorization. The appearance of German V-1 and V-2 guided weapons forced the British to confront entities which didn't conform to the launch, speed and trajectory profiles of manned bombers. Irregular Saddam Fedayyeen fighters engaged American forces during the advance on Baghdad in 2003, but they were invisible on Global Command and Control System plots which only displayed conventional Iraqi Army and Republican Guard units.[8] The ensuing counterinsurgency effort, with its focus on rebuilding the Iraqi state, required Americans to start tracking all kinds of urban planning variables not included in their operational metrics for the invasion. The introduction of new weapons can also push a military to pay attention to new types of things. As a general rule, the ability to strike more precisely requires that a military track more types of things. It is not enough to track a surface-to-air missile site once the launchers, radars, command vans, and decoys become separate targets that facilitate different objectives like hard-killing missiles or blinding radars. Beyond the identity of types, their stability is also a problem. If formations tend to stay together, then they can be represented with a single symbol. If they break into detachments, then more symbols of different types are needed. Particular ships, airplanes, and tanks are consolidated pieces of hardware that don't break into functional pieces. Composite units such as fleets or ground formations can divide and disperse. Emergent or unstable types of entities increase information friction.

4.2.1.2 Properties

The ontology might track the right types of things but not all of their relevant properties. New sensors or weapons might require as inputs details of construction that weren't counted before. Political considerations might arise to restrict targets with certain characteristics. For example, a target list might be assembled with an eye only to functional damage, but later on, political leadership requires special approval of targets with collateral damage estimates higher than some level of civilian casualties. Emergent or unstable properties raise information friction.

---

of that Map, inhabited by Animals and Beggars; in all the Land there is no other Relic of the Disciplines of Geography.

[8] Michael R. Gordon and Bernard E. Trainor, *Cobra II: The Inside Story of the Invasion and Occupation of Iraq* (New York: Random House, 2006), 314

4.2.1.3 Affiliation

Affiliation is a particularly salient property of battlefield entities. Is the world sorted into clean categories of friend, foe, and noncombatant? Do enemy forces wear uniforms and have identifying decals on their equipment? Or do combatants disguise their identity through stealth and subterfuge? Insurgents sometimes don police uniforms to infiltrate checkpoints. The Red Cross symbol should be a sacrosanct indicator of protected medical personnel, but unscrupulous foes use hospitals and ambulances to conduct hostile operations. Covert operatives deliberately forge identity documents and hide allegiances in order to penetrate enemy lines. Furthermore, loyalty can be more fundamentally uncertain. Alliances dissolve and insurgents switch sides. Spies are "flipped" to become double-agents. Combatants discard their uniforms and melt into civilian populations. Civilians and local officials provide information and material support to different factions as the neighborhood balance of power and availability of bribes shifts. When actors' loyalty and level of participation is questionable, then sophisticated data models and analysis can only estimate an unstable truth, which leads to information friction.

4.2.1.4 Relationships

Relationships give meaning to ontologies by describing constraints on how different entities correlate in space, time, and logic. Authority relationships in a chain of command, distribution channels in a narcotics network, physical connections in a power grid, kinship lines in a clan, and maneuver templates of ground units are all examples of relationships among entities.[9] Relationships are like entities in that they can be of a certain type such as marriage, business, or rival, and they have properties such as duration or strength. The same problems of emergent and unstable types and properties also apply to relationships; additionally, they can have problematic references to the entities related (thus a one-to-one communicative relationship might actually be a multilateral conference) or multiple overlapping relationships (as in an individual with "many hats" or titles in different organizations).

4.2.1.5 Number

In general, many types of entities, many properties of types, many types of relationships among entities, or large numbers of things themselves (*instances* of types) will increase information friction. With more things to track come more possible states of representation and

[9] I will collapse the notions of action and relationship together for simplicity. An action is a functional relationship between inputs and outputs. Some computational ontologies break out methods and actions separately.

thus more sources of equivocation. When confronted with a swarm of boats or aircraft, targeting systems face a harder triage challenge than with just one or two incoming contacts, especially if they have to differentiate hostile targets from neutral bystanders. In practice, numbers often count aggregate measures such as number of divisions instead of number of soldiers, which means that a lot of internal variance gets left out. Counterterrorist analysts usually model a network at the level of individual operatives, and yet the total number of people in a network is usually only a ballpark estimate; thus many instances of known types as well as previously unknown types might be hidden in the gap. When analysts or machines must decide how to categorize data given many choices, there is greater chance of miscategorizing. Metadata introduces additional properties to track for any record. Parsimonious models are easier to compute, while large numbers of types or instances of types complicates computation. Large numbers, furthermore, are often inflated in politicized debates over casualties and illicit traffic.[10]

4.2.1.6 Operational Domain

The complexity and number of types, properties, and relationships varies with the physical location of the battlefield. People don't permanently live at sea or in the air or outer space, and they require expensive technology to visit. Compared with cluttered ground environments full of variegated terrain, urban infrastructure and social flux, the ocean and the atmosphere are more homogenous media. Fewer numbers and types of entities of military import move around in them. Projectiles that overshoot targets at sea splash harmlessly, while ground fires carry risk of collateral damage. Ships, airplanes and satellites are not dispersed like ground forces, and less likely to change affiliation. The physical geometry of civilian aircraft and merchant vessels, as well as international protocols for tracking, simplifies identification. In comparison to cluttered terrestrial geography, representations of sea and aerospace can be more easily cleaned up into an exclusively military domain of threats and targets. The relative emptiness of the surrounding environment and the point-target nature of airplanes and ships lend themselves to abstract mathematical modeling. Even while objects may travel at high speeds at sea or in aerospace, their ontology remains relatively stable, and their trajectories are more likely to be mathematically estimable. This aspect of external stability promotes U.S. command of the commons, as discussed in the previous chapter.

---

[10] Peter Andreas and Kelly M. Greenhill, *Sex, Drugs, and Body Counts: The Politics of Numbers in Global Crime and Conflict* (Ithaca NY: Cornell University Press, 2010)

Note that ease of representation does not mean ease of fighting. War at sea can be far more risky than on the ground because it stakes large gambles on a few hefty capital investments. Winston Churchill famously described Admiral John Jellicoe, commander of the Royal Navy's Grand Fleet during the First World War, as "the only man on either side who could lose the war in an afternoon."[11] States and industries invest a lot of effort to stabilize the types and durability of equipment for high-leverage environments where little else survives. War at sea is easier to represent for the same reasons that it is more costly.

4.2.1.7 Geography

The ground environment is not unbridled chaos. Within the land domain, cluttered urban areas are harder to model than open "tank country." Terrain maps—*if* they adhere to cartographic standards and *if* they have been updated in some reasonable timeframe—tend to be reliable because mountains and coastlines do not shift radically, barring tectonic cataclysm. Rivers do indeed dry out, vegetation patterns change, and important tactical variation can be lost in the scale of terrain maps, as U.S. troops discovered in the unexpectedly corrugated washes in Afghanistan's Shahi-khot Valley during Operation Anaconda.[12] Nevertheless, geographic processes occur slowly enough that geographic patterns tend to be stable on tactical timelines.

4.2.1.8 Engineered Infrastructure

As suggested in the example of airline reservations, much stability is deliberately achieved through institutional work. Engineers create road and rail networks, cellular communications, and power grids by using standardized components and procedures. To the degree that these systems perform reliably without malfunction, then representations of systems will map well onto the structure of systems themselves. Telephones place calls to other telephones, and power substations connect to other stations, so the links and nodes of a network diagram of these systems can be given a relatively clear and stable interpretation. By contrast, diagrams of social networks or of any system with nonstandardized parts and haphazard connections have less stable mappings.[13] Structured infrastructures durably constrain the activities of militarized groups on the ground. While the high-resolution ontology of an

---

[11] http://www.royalnavy.mod.uk/history/naval-leaders/john-jellicoe (accessed 19 October 2010)

[12] Sean D. Naylor, *Not a Good Day to Die: The Untold Story of Operation Anaconda* (New York, NY: Berkley Books, 2005)

[13] Noah Shachtman, "How Technology Almost Lost the War: In Iraq, the Critical Networks Are Social—Not Electronic," *Wired* (27 November 2007)

insurgency amidst the population may be ambiguous, the contours of insurgent interaction amidst public infrastructure need not be. Geography and infrastructure provide stable frameworks which counterterrorism analysts use to triangulate more elusive clandestine patterns. Fractured geography and dilapidated infrastructure undermine the stability of that framework.

4.2.1.9 Social Structure

By the same reasoning, social institutions also constrain militarized groups. Families, clans, tribes, or organizational cultures are not changed overnight. Just as engineered infrastructures are ontologically durable, so too bureaucracies impose organization on their operations and use their own internal representations to do so. Unfortunately, the sources and extent of social stability remain active social science research topics (and probably always will), so it's never certain that explicit constraints in a model actually constrain a society. Nevertheless, more robust and stable institutions—like a professional military in a modern state—can support modeling more readily than a fissiparous anarchy on a lawless frontier.

4.2.1.10 Ontological Stability

To sum up the problem of battlefield ontology, some issues are more amenable to reliable representation than others. Proscribed worlds with well-defined types of and durable relationships among things are sweet problems for IT. By contrast, dirty volatile battlefields raise information friction because it is hard to know what types of things matter, how to categorize things, and when or whether those things have changed. Most actual operational environments feature subproblems with stable ontologies depending on the domain of conflict, the durability of engineered infrastructure, and the stability of social institutions. The overall relationship among subproblems is usually much messier.

4.2.2 Technical Possibility

The regularities of physics and the technical state of the art constrain whether or not it is even possible in principle to construct reliable cascades of inscription.[14] When important battlefield entities remain simply out of reach, or it is impossible to update the structure of representation at the rate the world changes, then information friction is heightened. By the

[14] Standard constructivist qualifications apply to the effect that scientific and technical facts are never simply given but have to be discovered and stabilized through a historical process of trial and error and resolution of controversy. The realist can rightly reply that material things are constrained by the material world, even if we don't understand exactly what those constraints are.

same token, the ability to connect farther and faster makes it possible in principle to stabilize a more complex and dynamic ontology, which lowers information friction.

Table 4-2: Intelligence Disciplines

Discipline	Description
Signals (SIGINT)	Emissions of electronic devices (ELINT) and human-to-human communications (COMINT); the distinction between the two is obscured somewhat in the emerging SIGINT discipline of computer network exploitation.[15]
Imagery (IMINT)	Terrestrial or airborne photography (PHOTINT) and satellite reconnaissance, increasingly referred to as geospatial intelligence (GEOINT) to include the fusion of remote imaging and digital cartography.[16]
Acoustic (ACINT)	The use of sound reflections to map undersea terrain and track submarines.[17] Used on land to detect the direction of gunshots and approaching vehicles.
Measurement and signature (MASINT)	A catchall term for more esoteric exploitations of explosive detonation signatures, missile telemetry data, human biometrics, multispectral change detection, *etc.*[18]
Human source (HUMINT)	Clandestine espionage, interrogation, and counterintelligence. Increasingly combines many of the other technical disciplines as agents can emplace sensors, collect precise coordinates, conduct computer network operations, *etc.*[19]
Open source (OSINT)	Academic, journalistic, government, corporate, and other information publically available for free or purchase. This category highlights the degree to which the military environment increasingly includes countless representations located well downstream from physical transduction, through one of the above methods, in other actors' cascades of inscription.[20]

[15] James Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency from the Cold War Through the Dawn of a New Century* (New York, NY: Doubleday, 2001); Robert J. Hanyok, *Spartans in Darkness: American SIGINT and the Indochina War, 1945-1975* (Ft. Meade, MD: Center for Cryptologic History, 2001). On capabilities and limitations of computer network operations see Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge University Press, 2007)

[16] John Diamond, "Re-Examining Problems and Prospects in U.S. Imagery Intelligence," *International Journal of Intelligence and Counterintelligence* vol. 14, no. 1 (2001): 1-24; Dwayne A. Day, *Eye in the Sky: The Story of the Corona Spy Satellites* (Washington, DC: Smithsonian Institute, 1999); on both IMINT and SIGINT satellites see Jeffrey T. Richelson, *America's Space Sentinels: DSP Satellites and National Security* (Lawrence, KS: Kansas University Press, 2001)

[17] Christopher A. Ford and David A. Rosenberg, *The Admirals' Advantage: U.S. Navy Operational Intelligence in World War II and the Cold War* (Annapolis, MD: Naval Institute Press, 2005); Owen R. Cote, "The Third Battle: Innovation in the U.S. Navy's Silent Cold War Struggle With Soviet Submarines," *Naval War College Newport Paper*, no. 16 (2003)

[18] Jeffrey Richelson, "MASINT: The New Kid in Town," *International Journal of Intelligence and Counterintelligence* vol. 14, no. 2 (2001): 149-192

[19] I. E Prikhodko, *Characteristics of Agent Communications and of Agent Handling in the United States of America* (San Francisco, CA: Interservice Publishing, 1981); Frederick Porter Hitz, *The Great Game: The Myths and Reality of Espionage* (New York, NY: Vintage, 2004); Robert Wallace, H. Keith Melton and Henry R. Schlesinger, *Spycraft: The Secret History of the CIA's Spytechs from Communism to Al Qaeda* (New York, NY: Dutton, 2008)

[20] Hamilton Bean, "The DNI's Open Source Center: An Organizational Communication Perspective," *International Journal of Intelligence and Counterintelligence* vol. 20 (2007): 240–257

For most of human history, records could circulate no faster than animal muscles or the wind could carry them. Clausewitz's disdain for intelligence was sensible given the low bandwidth of horseback messengers and the changeability of the battlefield between communications. In a famous instance two weeks after the Treaty of Ghent ended the War of 1812, the Battle of New Orleans was fought because the news had not arrived by ship from Britain, and thus the opposing commanders believed they were still at war. The growth of technical intelligence only took off with the ability to connect across distances with the telegraph. Twentieth century scientific progress in electromagnetism, acoustics, and mathematics, along with the industrial exploitations of these principles, enabled many new prosthetic modalities of sensation (Table 4-2).[21] The technical state of the art of those capabilities places an upper bound on the illumination of dead space. It also bounds how far out friendly forces can be tethered in space and time.

In order for technologies of connection to be usable, it must also be possible to move and transform records. The incorporation of advanced sensors and digital displays into ground combat vehicles had to await the invention of solid state transistors because vacuum tubes proved too fragile for punishing battlefield environments. In contemporary Afghanistan, sturdy laptops make it possible for Air Force tactical controllers to measure precision coordinates of pop-up targets in the field and pass them to combat aircraft overhead, which essentially moves a targeting center of calculation forward into the mud.

The technical state of the art does not determine a style of operations, but it does set bounds on what is possible. During World War I, control of infantry once they left the trenches was basically impossible because artillery chewed up telephone wires. Without reliable articulation cascades, commanders during the great battles of 1916-17 developed rigid timetables of bombardment and infantry advance which proved disastrously inflexible. The infiltration tactics that lead to the breakthroughs of 1918 did not change this hard constraint on the inability of headquarters to control the tactical battle. Instead, specially-trained "storm troops" initiatively bypassed and cut off strongpoints that follow-on infantry could mop up. Artillery pre-registered

[21] An accessible primer to modern intelligence disciplines and the U.S. intelligence community is Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington DC: CQPress, 2000). With more emphasis on information systems see Michael Herman, *Intelligence Services in the Information Age: Theory and Practice* (London: Frank Cass, 2001); Gregory F. Treverton, *Reshaping National Intelligence in an Age of Information* (New York, NY: Cambridge University Press, 2001)

targets to keep the element of surprise, and then advanced behind troops who communicated via colored flares and trailing observers, enabling artillery to be more selective in real time against points of resistance. Because long-range headquarters control was impossible, infiltration doctrine essentially broke the problem down into smaller problems where local control was possible with the visual signaling means then available.[22]

Advances in the technical state of the art can illuminate dead space. However, the ability to see more also increases the number of places to look to find anything, as well as the number of things the enemy might do to avoid being found or effectively engaged. Technology's effect on information friction is indeterminate when such interaction is taken into account. But all things being equal, some technical potential for connection and transmission of records at least provides a principled chance of setting up reliable cascades of inscription to lower information friction.

4.2.3 Enemy Action

War is finally a contest between adversaries. The enemy is ultimately the most important component of the information problem. As a willful combatant, the enemy tries to prevent control loops from closing and is thereby a potent force for destabilizing the problem.

4.2.3.1 Predictability

An enemy that adheres to doctrinal concepts or follows regular habits of life enhances the stability of the battlefield. Predictability makes reliable dead reckoning possible, which enables unsurprising reconnection with the enemy for intelligence collection or tactical engagement. The discussion of battlefield ontology above highlighted many instances of enemies complicating the stability of types, properties and relationships. Unpredictable enemies create ambiguous ontologies, while "cooperative" enemies lower friction. Predictability is not totally the enemy's choice, as he must also work within stable social, geographic, and technical constraints, like the facts that engines generate infrared signatures and corners reflect radar energy.

4.2.3.2 Attacks on Information Systems

Distributed cognition is a material process vulnerable to enemy action. Cover, concealment, and counterintelligence impede the creation of records of contact in the first place. Direct attacks on sensors, communications, or centers of calculation wreck the handling of

[22] Martin Van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985), 148-188. Although I don't develop the idea in this project, infiltration is essentially a type of expedient adaptation which required skilled soldiers with modular organic capabilities that they could mix and match for local circumstances.

records. Deception and propaganda inject misleading or manipulative records. To the extent that attacks on friendly information systems are relentless and systematic, friction increases.

For enemy attacks to be successful, they must exploit physical or logical vulnerabilities of friendly information systems. Physical and information security measures improve network performance and reliability even under attack. Weak defenses and single points of failure, by contrast, improve the odds that the enemy can strike effective blows against critical nodes. Criminals, spies and insurgents must especially guard their communications from intense counterintelligence attention, so they tend to use symbolic systems that are costly to mimic.[23]

This obvious point about security comes with an important caveat. An organization's own measures to harden its information systems impose costs on its own operations. Unwieldy classified information systems, inconvenient access control, physical hardening of workspaces, and avoidance of enemy monitoring all sap the reach and efficiency of friendly information flows. When terrorists rely only on couriers it might not be possible to track them through the telephone system, but the fact of surveillance denies them an ability to coordinate action at a distance and restricts their freedom. Usage of couriers and dependence upon the initiative of local agents introduces problems of principal-agency which can undermine their objectives and create internal feuds. The practice of "emissions control" risks "EMCON suicide."

4.2.3.3 Offense/Defense

Low-tech adversaries have proved able to frustrate U.S. forces in contested zones, but the only way for Americans to fight there is to go on the expeditionary offensive. America has abundant defensive security, but its forces can be frustrated overseas.[24] Local actors fight in defense of vital interests and thus are more willing to suffer. America's adversaries tend to have a plentiful supply of military-aged males to mobilize. They know the local terrain and society and can exploit it for cover and concealment. American expeditionary adventures in past decades have provided a laboratory for studying and devising countermeasures for the American way of war. Deadly weaponry for close fighting—explosives, assault rifles, and shoulder-

---

[23] Diego Gambetta, *Codes of the Underworld: How Criminals Communicate* (Princeton, NJ: Princeton University Press, 2009)

[24] Eugene Gholz, Daryl G. Press and Harvey M. Sapolsky, "Come Home, America: The Strategy of Restraint in the Face of Temptation," *International Security* vol. 21, no. 4 (1997): 5-48

launched missiles—is cheaply and widely available.[25] Widely available commercial software and the internet are a boon to adversaries' communications, intelligence, and recruiting.[26] Clausewitz points out that the attacker must deal with greater political constraints and controversy than the defender, who has only the negative object of parrying the blow and surviving. The defender can trade space for time, allowing the attacker to make mistakes and become exhausted in an unfriendly environment which he poorly understands. The defender, moreover, can rely on murderous guerrilla resistance, which saps the attacker's morale and political will. In sum, the defender can impose debilitating levels of friction on the attacker along all of its dimensions: danger, exertion, uncertainty, breakdowns, and controversy.[27]

Clauswitz's belief that defense is the stronger form of war suggests a tentative hypothesis that offensive operations generate more information friction. Defensive internal lines provide control over cascades of inscription and space for centers of calculation, whereas offensive external lines must push them into contested zones. I say tentative because one of the reasons why military organizations generally prefer offensive doctrines is that they allow them to control uncertainty by choosing a plan of attack that supports their own organizational processes while at the same time denying the defender his favored scenario.[28] That is, offensive doctrines are designed to lower information friction for one's own forces while raising it for the enemy. But in its complexity and vulnerability to unintended consequences, offense may do just the opposite.

4.2.3.4 Enemy Information Friction

It is better to fight a befuddled and capricious adversary than a perceptive and systematic one. The enemy's information friction is a boon, whether generated by internal pathologies or one's own efforts to deceive and degrade the enemy's distributed cognition. Kenneth Pollack attributes the consistently poor performance of Arab armies to "poor tactical leadership, poor information management, poor weapons handling, and poor maintenance,"[29] all of which

---

[25] Barry R. Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security* vol. 28, no. 1 (2003), 22-24

[26] Kelly Hearn, "Terrorist Use of Google Earth Raises Security Fears," *National Geographic News*, 12 March 2007; Bruce Hoffman, "The Use of the Internet by Islamic Extremists," Testimony to the House Permanent Select Committee on Intelligence, 4 May 2006; Jarret M. Brachman, "High-Tech Terror: Al-Qaeda's Use of New Technology," *The Fletcher Forum of World Affairs* vol. 30, no. 2 (2006): 149-164

[27] Clausewitz, *On War*, Book VI; Sumida, "Decoding Clausewitz," 153-175

[28] Barry R. Posen, *Sources of Military Doctrine: France, Britain and Germany Between the World Wars* (Ithaca, NY: Cornell University Press, 1984), 47-48

[29] Kenneth M. Pollack, *Arabs At War: Military Effectiveness, 1948-1991* (University of Nebraska Press, 2004), 574

contribute to breakdowns in control systems. The problems of relative information friction are worthy of developing more than I have the space to do here.[30]

Table 4-3 summarizes hypotheses on how external stability affects information friction.

Table 4-3: Hypotheses on the effect of external stability on information friction (XS→IF)

External Stability		Lowers Information Friction ↑	Raises Information Friction ↑
XS1.	Battlefield Order	Clean, Homogenous	Dirty, Cluttered
XS2.	Ontology	Simple, durable, distinguishable	Complex, changeable, ambiguous
XS3.	Combatant affiliation	Fixed, declared	Fickle, disguised
XS4.	Number	Few types and instances of types	Many types and instances
XS5.	Domain of combat	Air, Sea, Space	Ground
XS6.	Connection to entities	Technically possible to reach out and contact across long distance	Inaccessible entities
XS7.	Movement of records	Technically possible to securely and quickly transport records	Incommunicable records
XS8.	Enemy behavior	Cooperative, predictable	Frustrating, deceptive
XS9.	Enemy attacks on information system	Haphazard, uncoordinated	Determined, systematic
XS10.	Exposure of system	Hardened, redundant, "operational security"	Vulnerable, single points of failure, "EMCON suicide"
XS11.	Offense/defense	Defense ("stronger form of war")	Offense
XS12.	Information friction in enemy system	High (confused enemy)	Low (intelligent enemy)

4.3 Internal Consensus in the Bureaucracy

The second major cause of information friction is internal consensus. External stability concerns the problem an information system tries to solve, and internal consensus concerns the way it goes about solving it. While the nature of the battlefield generates friction, militaries also generate it internally. Organizational politics can hobble their ability to implement effective solutions regardless of the stability of the objective problem. Modern forces are composites of many units hailing from different services, executive agencies, and alliance partners. Each of these has sub-organizations. IT connects them and can facilitate their cooperation or conflict. Thus the adoption of technical protocols becomes an unavoidably political process rather than just an engineering question. Hopeful technocrats often assume away the political problems by

[30] Barry D. Watts, "Clausewitzian Friction and Future War, Revised Ed." National Defense University, McNair Paper, no. 68 (2004), mentions the importance of relative friction over absolute certainty.

advocating "enterprise solutions" and "interoperable frameworks." But *interference* and *insulation* are also potential outcomes. Excessive internal consensus with a lack of external stability will generate the insulation variety of information friction. Otherwise, insufficient consensus regardless of external stability creates the interference variety. Both will be fleshed out further below.

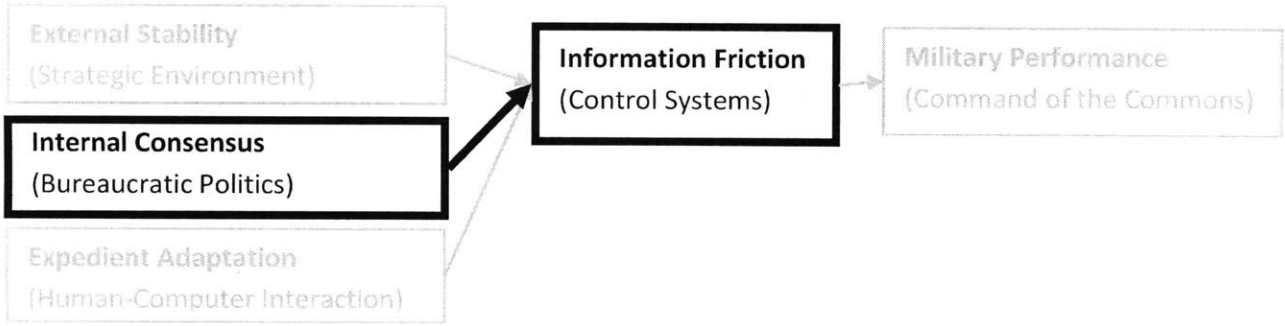


Figure 4-2: Causal relation between internal consensus and information friction

4.3.1 Doctrinal Agreement

Barry Posen describes military doctrine as "a set of prescriptions…specifying how military forces should be structured and employed to respond to recognized threats and opportunities" and a specification of "modes of cooperation between different types of forces." Doctrine thus answers two questions: "*What* means shall be employed? and *How* shall they be employed?"[31] Forces that are unable to answer these questions or that are composed of components that answer them in incompatible ways will experience high information friction. If the definition of the computational problem is politicized, then different organizations will end up implementing incompatible representational architectures. The political makeup of shareholders in any given representational scheme can vary along the following lines to raise or lower friction.

4.3.1.1 Organizational Preferences

Military organizations usually have strong opinions about what is militarily possible and what is the best way to attack a problem. These preferences can be stated in doctrinal publications and mission statements, but they are usually expressed more strongly in the way an organization spends its money, buys its weapons, and trains its people. Stated preferences and expressed preferences can and often do diverge. For example, all of the American services

[31] Posen, *Sources of Military Doctrine*, 13

stated a desire for RMA "transformation" after the Cold War, but their procurement patterns expressed largely more of the same.[32] Different services have different cultures rooted in their historical operating environments, so that, to make some gross generalizations, the Navy takes pride in its institutions and autonomy, the Army takes pride in its loyalty to the mission, and the Air Force takes pride in its technical capabilities.[33] Furthermore, each of the services have different subcultures built around particular missions and weapon systems, such as the "brown shoe" naval aviators and "black shoe" surface warfare officers who cohabitate aboard aircraft carriers with some mutual disdain.[34] Parochial subcultures often have different opinions on the best goals to pursue and proper ways to man, train and equip for war. Furthermore, military organizations are particularly "value infused," so the maintenance of organizational essence and reenactment of organizational lore become so fundamental to members' identity that they can displace rational consideration of the mission.[35]

Information friction increases when interdependent organizations or suborganizations have divergent ideas about their military or political goals. Consensus about doctrinal goals lowers it except when parochial preferences are misaligned with the operational situation.

4.3.1.2 Number and Size of Stakeholders

The more actors that have a stake in any given representational scheme, the more likely their private interests will diverge. Desirable IT qualities like security, reliability, interoperability, organized files, common ontologies, and search efficiency are public goods for a community of users. Likewise, many of the most frustrating everyday problems in organizational computer use are actually commons problems. Email boxes fill up with low-priority traffic, the organization of the shared file server becomes inscrutable, the meaning of database fields becomes ambiguous, and personnel struggle to align incompatible systems.

---

[32] Harvey M. Sapolsky, Benjamin H. Friedman and Brendan Rittenhouse Green, *U.S. Military Innovation After the Cold War: Creation Without Destruction* (New York, NY: Routledge, 2009)

[33] Carl Builder, *The Masks of War: American Military Styles in Strategy and Analysis* (Baltimore, MD: Johns Hopkins University Press, 1989); Austin G. Long, "First War Syndrome: Military Culture, Professionalization, and Counterinsurgency Doctrine," Ph.D. dissertation, Massachusetts Institute of Technology, 2010

[34] Roger Thompson, "Brown Shoes, Black Shoes, and Felt Slippers: Parochialism and the Evolution of the Post-War U.S. Navy," U.S. Naval War College Center for Naval Warfare Studies Occassional Paper, 1995

[35] Phillip Selznick, *Leadership in Administration: A Sociological Interpretation* (Evanston, IL: Row, Peterson and Co, 1957); Paul J. DiMaggio and Walter W. Powell, "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality," in *The New Institutionalism and Institutional Analysis*, ed. Walter W. Powell and Paul J. DiMaggio (Chicago: University of Chicago Press, 1991): 63-82

Individual users appropriate IT for their own needs while contributing little to public representational goods, unless a manager makes them adhere to standards. Mancur Olson explains that in the absence of coercive authority, public goods tend to be underprovided, diffuse interests underrepresented, and concentrated interests overrepresented.[36] We should thus expect fragmented and turbulent communities of actors to produce messy information systems. Also, systems with disparities in political clout should distort information systems to serve the interests of the most bureaucratically empowered.

4.3.1.3 Autonomy

Organizational autonomy is one sure way to achieve consensus over preferences and to ensure that means are brought into alignment. Insofar as autonomy enhances distributed cognition, it also improves an organization's control over uncertainty. The bureaucratic pursuit of autonomy, identity, control, and wealth are intertwined.[37] For the organization in question, autonomy lowers information friction, and thus "unity of command" is a much-vaunted principle of war. However, at higher levels of analysis, autonomy can also manifest as insulation if organizations work at cross purposes to the larger whole.

4.3.1.4 Division of Labor

Few military organizations are truly autonomous (the Lewis and Clark expedition comes to mind). The division of labor is essentially a bureaucratic abstraction which breaks tasks down into black boxes defined only by their functional inputs and outputs. Many centers of calculation share the burden of computing representations in complex command and control. If bureaucratic interfaces are well defined; if work is rationally partitioned across centers with a minimum of informal negotiation; and if stakeholders stay in their "lanes in the road," then they will be able to share information and construct stable representations. Ill-defined, overlapping, and contested divisions of labor will translate into leaky abstractions.

4.3.2 Political Control of Technical Standards and Protocols

The configuration of actors just described has to choose and implement data-management protocols. Common standards promote interoperability and improve control, but for the same

---

[36] Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups, 2nd Ed.* (Cambridge, MA: Harvard University Press, 1971); Kenneth A. Oye, ed., *Cooperation Under Anarchy* (Princeton, NJ: Princeton University Press, 1986)

[37] Morton H. Halperin, *Bureaucratic Politics and Foreign Policy* (Brookings Institution Press, 1974)

reason they provide competitive advantage, which makes defining and adopting them a political problem.[38] Common railway gauges facilitate trade across borders as well as invasion. The politics of standards especially plagues IT because it is a technology literally built out of layer upon layer of hardware standards and software protocols.

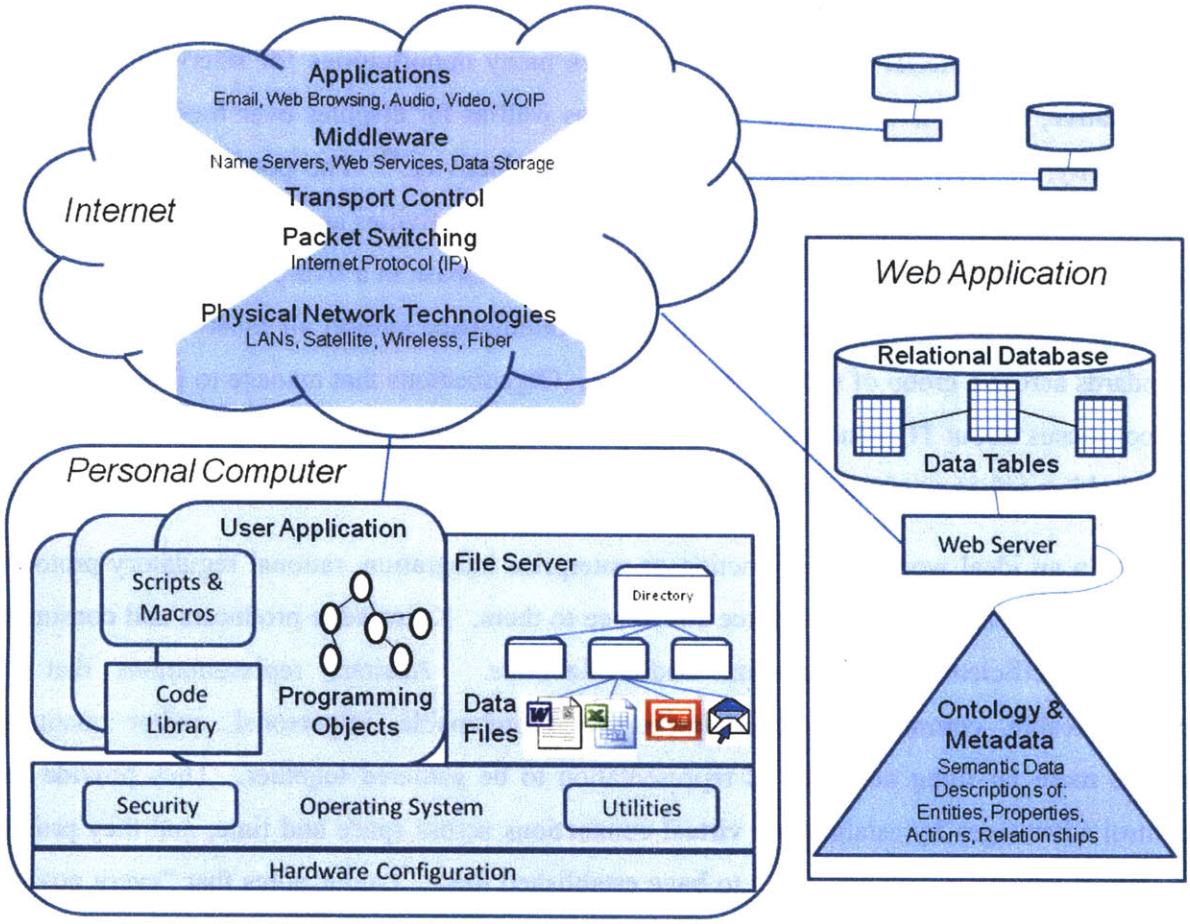


Figure 4-3: A sketch of the complex layering of modular abstractions which compose modern IT

Figure 4-3 depicts some of the abstractions that form the building blocks of contemporary IT: the "internet hourglass" shows how internetworking protocols (TCP/IP) insulate useful applications from the physical implementation of the network; the internet connects web servers running relational databases that communicate their semantic structure to other web applications via a formal ontology or data dictionary; end users run applications built out of modular code

[38] Carl Shapiro and Hal R. Varian, "The Art of Standards Wars," *California Management Review* vol. 41, no. 2 (1999): 8-32; Martha Lampland and Susan Leigh Star, *Standards and Their Stories: How Quantifying, Classifying, and Formalizing Practices Shape Everyday Life* (Ithaca NY: Cornell University Press, 2009); Robert L. Mallett, "Why Standards Matter," *Issues in Science and Technology* (Winter 1998)

libraries and tailored scripts to read and write from their file system and the "internet cloud." No one organization controls and manages all of this. The layering and modularity of IT architecture supports a diverse menagerie of actors who make their living around the different parts: software engineers, internet service providers, government regulators, corporate managers, military officers, network administrators, end users, end users in other departments, *etc.*[39] The incredible combinatorial richness of IT provides many opportunities for intervention by both cooperative, competitive, and malicious actors, as well as for disputes over fundamental values of security, privacy, free speech, and economic productivity.[40] The potential for fights over representational protocols goes all the way down because activities as diverse as the use of a file naming convention, the adoption of an administrative database in a five-person work center, or a major decision to implement a new interagency intelligence system all must enforce common standards across a group of self-interested actors. Organizations that manage to forge some kind of consensus about IT standards and protocols will be able to lower information friction. If stakeholders refuse or are unable to harmonize standards then they will raise information friction.

In an ideal world of low friction or enterprise integration, rational regulatory protocols define stable abstractions and enforce adherence to them. Knowledge producers and consumers can then efficiently self organize and collaborate. Abstract representations that are communicable, commensurable, comprehensive, combinable, impersonal, and/or quantified enable more far-flung networks of representation to be gathered together. They provide real control advantages by establishing virtual connections across space and time, and they provide rhetorical advantages by appearing to have established them. Latour notes that "every possible

---

[39] David G. Messerschmitt and Clemens Szyperski, *Software Ecosystem: Understanding an Indispensable Technology and Industry* (Cambridge, MA: MIT Press, 2003). A nice review of the different kinds of layers in PCs, networks, and applications is found in Elihu Zimet and Edward Skoudis, "A Graphical Introduction to the Structural Elements of Cyberspace," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (Washington DC: National Defense University Press, 2009): 91-112

[40] Ithiel De Sola Pool, *Technologies of Freedom: On Free Speech in an Electronic Age* (Cambridge, MA: Belknap Press, 1983); David D. Clark, John Wroclawski, Karen R. Sollins and Robert Braden, "Tussle in Cyberspace: Defining Tomorrow's Internet," *IEEE/ACM Transactions on Networking* vol. 13, no. 3 (2005): 462-475; Jonathan L. Zittrain, "The Generative Internet," *Harvard Law Review* vol. 119, no. 7 (2006): 1975-2040; David D. Clark, "Network Neutrality: Words of Power and 800-Pound Gorillas," *International Journal of Communication* vol. 1 (2007): 701-708; Lawrence Lessig, *The Future of Ideas: The Fate of the Commons in a Connected World* (New York, NY: Random House, 2001)

innovation that offers any of these advantages will be selected by eager scientists and engineers,"[41] and the same can be said of eager bureaucrats and military officers.

Conversely, the definition of representational protocols that are incommunicable, incomparable, fragmented, confusing, idiosyncratic, and/or qualitative tends to increase information friction. The happy ideal of enterprise integration is vulnerable to two different types of failure. The *interference* variant of friction occurs when actors generate negative externalities and coordination failures.[42] The *insulation* variant occurs when protocols are captured by powerful rent-seekers and paralyzed by high transaction costs.[43] Any government or corporate organization struggles to capture the benefits of both decentralized markets and regulatory hierarchies and to avoid their characteristic failure modes.[44] Any sociotechnical system will involve a mixture of these forms: decentralized exchanges feature dense structure outside of the formal order of hierarchy, while formal bureaucracies have a lot of decentralized confusion inside.[45] The last chapter described the difference between interference and insulation only vaguely in terms of the closure of control loops. This section describes them in more depth in terms of the political economy of distributed cognition (Table 4-4).

---

[41] Bruno Latour, "Drawing Things Together," in *Representation in Scientific Practice*, ed. Michael Lynch and Steve Woolgar (Cambridge, MA: MIT Press, 1990), 47

[42] On market failure see: R. H. Coase, "The Nature of the Firm," *Economica* vol. 4, no. 1 (1937): 386-405; R. H. Coase, "The Problem of Social Cost," *Journal of Law and Economics* vol. 3 (1960): 1-44; Joseph E. Stiglitz, "Information and the Change in the Paradigm in Economics," *American Economic Review* vol. 92, no. 3 (2002): 460-501

[43] On regulatory failure see: Herbert Kaufman, *Are Government Organizations Immortal?* (Washington DC: Brookings Institution, 1976); Joseph E. Stiglitz, "The Private Uses of Public Interests: Incentives and Institutions," *Journal of Economic Perspectives* vol. 12, no. 2 (1998): 3-22; Terry M. Moe, "Political Institutions: The Neglected Side of the Story," *Journal of Law, Economics, & Organization* vol. 6, special Issue (1990): 213-253; Paul Milgrom and John Roberts, "An Economic Approach to Influence Activities in Organizations," *American Journal of Sociology* vol. 94 (1988): S154-S179; Amy Zegart, *Flawed by Design: The Evolution of the CIA, JCS, and NSC* (Stanford, CA: Stanford University Press, 1999)

[44] Oliver E. Williamson, "The Economics of Organization: The Transactions Cost Approach," *American Journal of Sociology* vol. 87, no. 3 (1981): 548-77; Oliver E. Williamson, *The Mechanisms of Governance* (New York: Oxford University Press, 1996)

[45] Mark Granovetter, "Economic Action and Social Structure: The Problem of Embeddedness," *American Journal of Sociology* vol. 91, no. 3 (1985): 481-510; Walter W. Powell, "Neither Market Nor Hierarchy: Network Forms of Organization," *Research in Organizational Behavior* vol. 12 (1990): 295-336

Table 4-4: Variance of information friction in terms of control and political-economy

Political Economy →	Information Friction	Control Loop Closure
Efficient knowledge markets with enabling regulatory institutions	Low: **Enterprise Integration**	Close on entities of concern (enemies or allies)
Decentralized market failure	High: **Interference**	Hung open
Political/regulatory failure	High: **Insulation**	Premature closure

4.3.3 Enterprise Integration

The achievement of internal consensus stabilizes information channels between organizational units and between the organization and its environment. There are different mechanisms for harmonizing technical standards across groups: direct hierarchical command, communal negotiation, or the dominance of standards through market competition. Militaries obviously use hierarchical bureaucratic means to enforce cooperation. However, they are also communities that negotiate over mutual monitoring and enforcement of decisions to use a given protocol.[46] Militaries also adopt IT from the commercial sector, in effect relying on the market domination of particular standards—such as Microsoft *Windows* and *Office*—to provide interoperability. However, an organization still has to choose and enforce standards even if they are market favorites, so there's really no escape from managerial intervention. It's beyond my scope to analyze these different harmonization processes in detail, so I will lump them all together as the achievement of some form of legitimate governance, be it consensual or coercive, over the information system architecture.

4.3.3.1 Management of Complexity

Integrated enterprises coordinate many different people and resources, and they provide economies of scale. A designated "lead system integrator" usually helms multi-stakeholder projects via frequent coordination meetings and detailed control schemes.[47] They manage many organizations, engineers, and materials over a long period of time. The efficient decomposition

---

[46] See the general logic in Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (New York, NY: Cambridge University Press, 1990), with application to information systems in Charlotte Hess and Elinor Ostrom, "Ideas, Artifacts, and Facilities: Information As a Common-Pool Resource," *Law and Contemporary Problems* vol. 66 (1/2 2003): 111-145; Charlotte Hess and Elinor Ostrom, *Understanding Knowledge as a Commons: From Theory to Practice* (Cambridge, MA: MIT Press, 2007). The community aspect of military organizations is stressed by Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca, NY: Cornell University Press, 1991)

[47] Thomas P. Hughes, *Rescuing Prometheus: Four Monumental Projects That Changed the Modern World* (New York: Vintage, 1998); Andrea Prencipe, Andrew Davies, and Michael Hobday, eds., *The Business of Systems Integration* (Oxford University Press: 2003)

of complex problems into simpler modular parts isolates design activity within compartments from design activity outside them.[48] Network managers and procurement officials establish network configuration rules, design requirements, and long-range resource management schemes to avoid the security, maintenance, and interoperability shortcomings of the interference variant of high information friction, discussed below. Unfortunately, this administrative overhead also risks the creation of the insulation variant, also discussed below.

Nicholas Argyres tells a sanguine story of how four different defense contractors used IT to coordinate construction of the B-2 stealth bomber. He describes efficient decentralized project governance, with a strong emphasis on rigid standards and development of a technical grammar which allowed for vertical disintegration and control of transaction and agency costs. Yet he also notes in passing that Air Force intervention to set process standards was critical. A common open framework can improve coordination, but coordinating and enforcing adherence to that framework itself is a costly governance problem.[49]

4.3.3.2 Semantic Interoperability

Sophisticated abstractions can provide both flexibility and referential integrity, but there is no way to escape the requirement for stakeholders to agree to adhere to standards at some point. Figure 4-4 shows different ideal options for connecting three different data stores, A-C, each with a different model of the world (The dark shapes are formal models of each system, with the superscript noting the location of the model.).[50] They might be databases of hotels, flights, and airports for a travel reservation system, each with overlapping data elements. Data models for each database could be mapped directly to one another or to an intervening common ontology, and the mapping could be performed centrally or by each system independently, which gives four types of semantic interoperability. On the top left, a central application maps each of the data models directly to the others. On the top right, the application maps each to an ontology, which enables changes to one model without also having to remap the others. On the bottom left, each database A-C internally maps into the others, which means that any change to

---

[48] Carliss Y. Baldwin and Kim B. Clark, *Design Rules, Vol 1: The Power of Modularity* (Cambridge, MA: MIT Press, 2000)

[49] Nicholas S. Argyres, "The Impact of Information Technology on Coordination: Evidence From the B-2 "Stealth" Bomber," *Organization Science* vol. 10, no. 2 (1999): 162-180

[50] For example, database A could contain flight schedules, B could contain information about specific models of planes, and C could contain information about airports. A web application looking to optimize flights for a customer would draw on all of them.

one model requires others to change their mappings too. On the bottom right, the designers of A-C all agree in advance on a single lingua franca to define their data. This last peer-to-peer option appears radically decentralized, but only because of a prior agreement to conform to a single ontology, which might become a problem if one wants to add new entities and relationships that don't fit.[51]

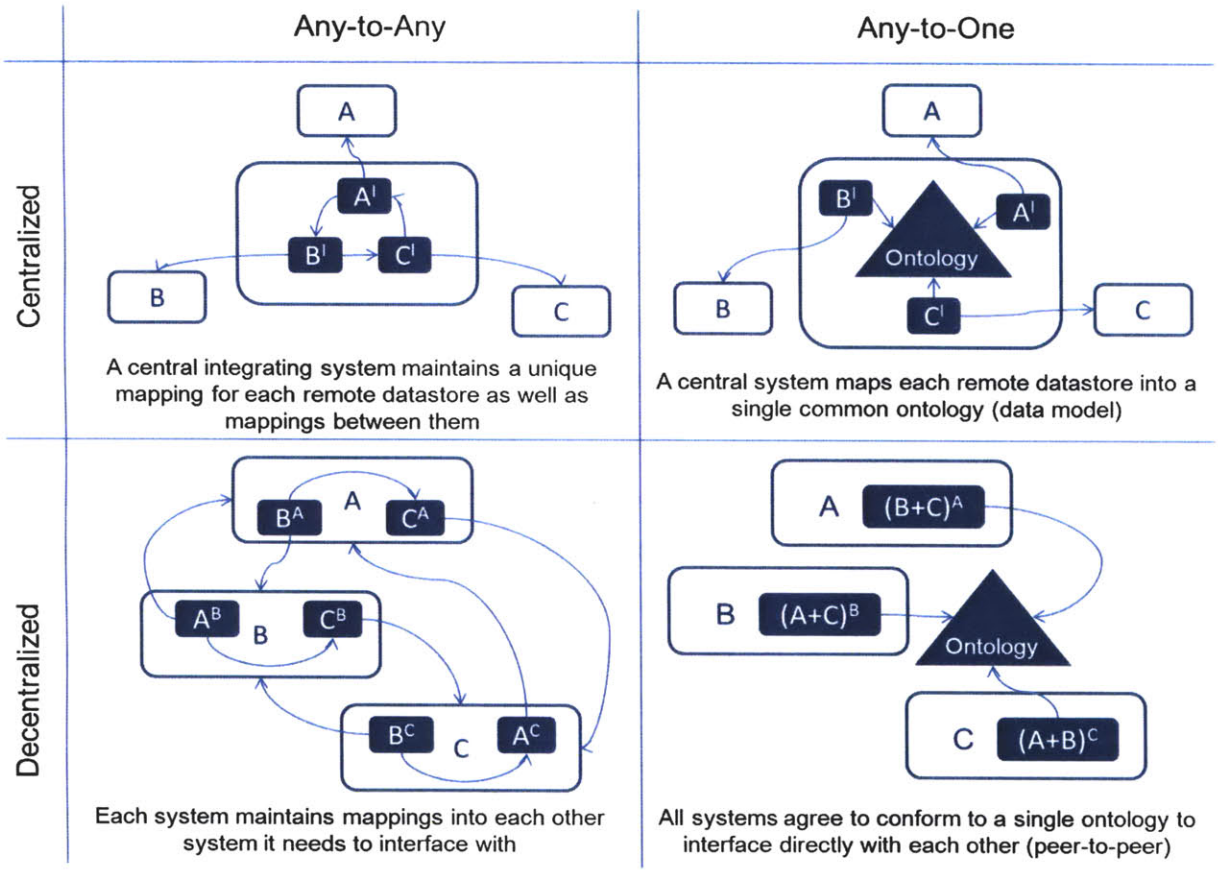


Figure 4-4: Models of semantic interoperability

All of these models of semantic interoperability require engineers to commit at some point to establishing standards with others. There can be no master ontology to exhaustively and formally describe all entities, features, and relationships in the world, as discussed earlier, but only pragmatic models of proscribed domains. Hope springs eternal that higher and higher levels of abstraction will enable harmonization, but that only demands consensus among more people at broader scales. Unless stakeholders agree to adhere to a common ontology in one of

[51] These distinctions and Figure 4-4 based on Guido Vetere and Maurizio Lenzerini, "Models For Semantic Interoperability in Service-Oriented Architectures," *IBM Systems Journal* vol. 44, no. 4 (2005): 887-904

these four ways, and thus lower information friction, then fragmented ontologies create a digital Tower of Babel.

4.3.3.3 Accountability

Enterprise integration enhances accountability by depersonalizing systems and improving the transparency of their construction. The establishment of data ownership, maintenance responsibility, and audit logs shift system reliability from individual persons to organizations. The same techniques that make the enemy more visible and controllable also provide the means to monitor an organization's members and enforce compliance with organizational policy. "Two person integrity" rules protect the handling of Top Secret data. Target review boards attempt to audit the identification of bombing targets and coordinate accuracy. Gun camera video provides forensic evidence to investigate or exonerate soldiers involved in shooting civilians. Multiple access protocols—passwords, ID cards, biometrics—enable security personnel to track the comings and goings of personnel to sensitive spaces to correlate their activity with events of counterintelligence concern. Such measures harden cascades of inscription against enemy disruption so that their end product in a center of calculation is trustworthy.

Stabilized systems that behave like black boxes are more trustworthy, especially if it's easy to open them up for inspection when something goes wrong. Unfortunately, personnel in them also become more risk-averse out of fear of making a legible mistake and getting punished. Accountable systems have less slack, discussed below under expedient adaptation, and they inadvertently create work-to-rule slowdowns, discussed below under insulation.

4.3.4 Interference

Organizations that fail to achieve the sort of consensus about protocols required for the sanguine behavior described above will raise information friction. The interference variant of friction occurs when the organization is unable to coordinate distributed cognition and experiences palpable breakdowns. Actors process information for their local or private problems, but in so doing, per the Olsonian dynamic described earlier, they generate negative externalities for others who have to share information or coordinate behavior.

4.3.4.1 Stovepipes

Organizational subunits procure or develop IT for their particular mission, but these "stovepipe" systems might not interoperate across subunits. Incompatibility ranges from radios

that can't physically connect; databases with austere classification or proprietary restrictions; conflicting formats of dates, times, geocoordinates, *etc.*; and non-orthogonal assumptions about what sorts of entities, properties, and relationships to track. Incompatible systems and data formats have been a recurring nightmare for military command and control for decades. The fragmentation of systems regularly defies attempts to rationalize them. Many high-profile military mishaps have highlighted information system disconnects and provided impetus for centralizing reforms such as failures to share data during the Bay of Pigs fiasco; communication relay failures in the Mayaguez incident; interservice coordination failure in the botched hostage rescue attempt in Iran in 1980; tactical communication failures in Granada; *etc.*[52]

4.3.4.2 Information Overload

Improvements at one level often just push problems up to another, classically from connectivity headaches to "information overload" problems. Improved connectivity makes it possible to gain access to more data of questionable provenance. It is one thing to recognize, as the Army chief of staff in 1980 said, "There is more information than we need. We must discipline ourselves to only get at the level of data needed to cause decisions to happen."[53] It's quite another to settle on that level when the quality and relevance of data is ambiguous, provenance is unclear, and the technical competence needed for such discipline is unevenly distributed. Advanced IT provides connectivity to more data of dubious value, or more charitably, valuable only within some specific local circumstances. Always in search of better needles, officers end up building bigger haystacks.

Recent cognitive science research suggests that the brains of remote vehicle operators can become sharply overloaded while dealing with multiple video information sources in combat scenarios, which can only be expected to be exacerbated by combat stress. After the accidental killing of 23 Afghan civilians by American gunships in February 2010, investigators found that Predator drone operators had solid information that the group included children but were unable to focus on it because of so many other pieces of data and demands on attention. A senior officer

---

[52] David E. Pearson, *The World Wide Military Command and Control System: Evolution and Effectiveness* (Maxwell, AL: Air University Press, 2000); C. Kenneth Allard, *Command, Control, and the Common Defense* (New Haven, CT: Yale University Press, 1990)

[53] Quoted in Allard, *Command, Control, and the Common Defense*, 137

said that the deaths might have been prevented "if we had just slowed things down and thought deliberately."[54]

4.3.4.3 Fratricide

Some of the most dangerous mutual interference problems are collisions, accidents, and "friendly fire" which result from the sudden connection of uncoordinated information systems, or failure to connect when needed. An apocryphal yet illustrative myth about the battle of Austerlitz is that Russian and Austrian forces aided Napoleon's victory by failing to converge as previously agreed because of their respective use of Julian and Gregorian calendars.[55] There have been severe targeting errors because of discrepancies in datum—the cartographic reference point mapping ellipsoid models to the real earth—between the maps of soldiers calling for fire and the maps of those delivering it. Thus the "same" grid coordinate derived from different datums could map onto the earth hundreds of yards or even miles apart.[56]

Scott Snook details how an Air Force airborne control crew, F-15 fighter pilots, and Army Blackhawk helicopters constructed locally consistent representations of their situation in Iraq in 1994. Each had relaxed formal procedures and adopted idiosyncratic practices in a decoupled state, but they assumed the others were still adhering to standard practices. The pair of Blackhawks had deviated from schedule; the airborne control aircraft had some inexperienced crewmembers and had relaxed data-checking protocols; the fighter pilots were primed to see Iraqi aircraft violating No-Fly Zone airspace. The controller thus cleared the F-15s to shoot down the Blackhawks, which both mistakenly identified as hostile Iraqi aircraft. The "practical drift" apart of local sensemaking practice suddenly recoupled in a tragic fratricide.[57] Diane Vaughan provides a similar explanation for the Challenger space shuttle disaster as a case of "normalized deviance" at NASA, where engineers and astronauts adopted idiosyncratic practices over time and failed to correct aberrations from standards because, most of the time, there was no

---

[54] Thom Shanker and Matt Richtel, "In New Military, Data Overload Can Be Deadly," *New York Times* (16 January 2011)

[55] Robert Goetz, *Austerlitz: Napoleon and the Destruction of the Third Coalition* (London: Greenhill, 2005)

[56] This problem has been largely relegated to U.S. military history with widespread convergence on the WGS-84 datum, but is still a risk with foreign maps.

[57] Scott Snook, *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks over Northern Iraq* (Princeton: Princeton University Press, 2000)

consequence to the shortcuts.[58] Leaky abstractions and local idiosyncrasies heighten the chance of accident when decoupled systems suddenly recouple.

4.3.4.4 Veracity Bubbles

When users can't tell the difference between well-constructed and invalid representations, organizational networks will have more suspect representations. In George Akerlof's "market for lemons," imperfect information causes bad products to drive out good: buyers can't discriminate quality, the market is flooded with inferior products, and reputable sellers exit the market.[59] When computer users can't tell the difference between secure and insecure software, the market tends to offer more insecure software.[60] Declining costs of graphic design undermine signals of reputable publishers : anyone with a computer can create attractive fonts, layouts and logos. Digital networks become echo chambers for decontextualized bullet points and catchy diagrams. Reliable knowledge—with known provenance and competent evaluation—is undervalued in a market for informational lemons.

As a result, many suspect intelligence claims or bad target nominations turn up again and again in new formats even after they have been censored. The same IT that empowers users to mix and match (or "mash up") digital products also empowers them to indulge in unbridled plagiarism and sloppy analysis by discarding audit trails that would enable one to evaluate knowledge claims. The reputational imprints of analytical agencies become suspect when analysts just cut and paste data from one document or PowerPoint slide into another. They change fonts and layouts but little of substance, and they discard provenance metadata along the way. Investigation into the reliability of the result is likely to be met with resistance, as if the analytical competence of the author is being questioned.

When metadata that is supposed to signify provenance loses its referential integrity, informational lemon markets can lead to dangerously distorted representations of the world. Consider the mortgage-backed instruments involved in the financial collapse of 2008. Some firms like Magnetar cynically bet on and helped perpetuate the crash, but the real problems were

---

[58] Diane Vaughan, *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA* (Chicago, IL: University of Chicago Press, 1997)

[59] George A. Akerlof, "The Market For "Lemons": Quality, Uncertainty and the Market Mechanism," *Quarterly Journal of Economics* vol. 84, no. 3 (1970): 488-500

[60] Ross Anderson, "Why Information Security is Hard: An Economic Perspective," 17th Annual Computer Security Applications Conference (2001): 358–365

caused by less sinister and more tragic pathologies. Highly-leveraged financial derivatives were difficult to accurately value because their construction drew on clusters of securities rated according to inconsistent criteria. Complex tranches which included extremely risky housing loans thus received AAA ratings. Densely connected financial networks, sophisticated tools for financial engineering, and physicists repurposed for Wall Street all combined into a perfect storm wherein highly-leveraged local adaptation generated tremendous systemic risk. Manic investors made locally rational decisions based on the representations before them, and the investment bubble grew until the inevitable panic and crash.[61]

Similarly, national intelligence is often difficult to evaluate because of source secrecy, complicated collection, and genuine uncertainty. Questionable reporting can be incorporated into further intelligence and decision products as provenance references are dropped. Analytical assessments can be compared to inscrutable bond ratings, compartmented behind security walls and compounded upon unauditable chains of prior assessments. Assessments become detached from any correspondence with reality, yet continue to trade with authority. Investment bubbles in the veracity of information form. The intelligence judgments surrounding the assessment of Iraq's weapons of mass destruction in 2002-3 appear to fit this pattern: a long series of reasonable judgments in their local context; an accumulating mass of glittering analytical products describing the overall chemical and biological programs; the failure to properly vet dubious sources like the HUMINT asset code-named "Curveball" due in part to security compartmentalization; and political pressure to produce a positive intelligence judgment. All contributed to substantial willingness to invest in the WMD hypothesis.[62] The magnitude of the intelligence crash became apparent only after the invasion of 2003 failed to find WMD. As before the financial crash of 2008, there had been Cassandras aplenty, but the bubble of toxic intelligence proved too tempting an investment for too many politically-interested actors.

---

[61] Donald MacKenzie, "The Credit Crisis as a Problem in the Sociology of Knowledge," Working Paper, September 2010, http://www.sps.ed.ac.uk/__data/assets/pdf_file/0019/36082/CrisisRevised.pdf (accessed 20 October 2010); See also Donald MacKenzie, *An Engine, Not a Camera: How Financial Models Shape Markets* (Cambridge, MA: MIT Press, 2006), which examines the role that finance theory and exchange automation played in precipitating the financial crises of 1987 and 1998.

[62] Robert Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca NY: Cornell University Press, 2010)

4.3.5 Insulation

Insulation is perhaps the more ominous sort of information friction because certain ways of seeing and dealing with the world get locked in. If the function of cascades of representations in distributed cognition is to connect and coordinate disconnected entities, here these information flows circle back onto themselves. They reproduce and amplify organizational preferences, filter out discrepant signals, and lock in behaviors that become counterproductive.

4.3.5.1 Rent-Seeking and Transaction Costs

Consensus on technical protocols must be backed up by adequate and focused investment to implement them, obviously, in order to realize an integrated enterprise. However, military command and control is so expensive—the Department of Defense reportedly requested $43.3 billion for 2011[63]—that the management its costs and complexity increases friction. Weapons procurement is notoriously inefficient. Tremendous transaction costs arise from demand-side uncertainty in the strategic environment (what wars will we fight and how will we fight them?) and supply-side rent-seeking within the "iron triangle" of congress, the military, and the defense industry. A dense thicket of acquisition regulations and lobbying relationships stand between doctrinal concepts and actual weapons. Established contractors seek competitive advantage in negotiating red tape and lobbying policymakers as much as they do in engineering weapons, which forms a barrier to entry for new firms and user innovators. Approved contracts emerge from a costly bargaining process of logrolling among congressmen and the services themselves.[64] The monopsony, secrecy, uncertainty, and huge financial sums involved in

---

[63] "Defense Funding for C4ISR Remains Stable," Defense Talk blog (23 June 2010), http://www.defencetalk.com/defense-funding-for-c4isr-remains-stable-27176/ (accessed 22 October 2010)

[64] Harvey M. Sapolsky, Eugene Gholz and Caitlin Talmadge, *US Defense Politics: The Origins of Security Policy* (New York, NY: Routledge, 2008), 61-95; Peter J. Dombrowski and Eugene Gholz, *Buying Military Transformation: Technological Innovation and the Defense Industry* (New York, NY: Columbia University Press, 2006); Gordon Adams, *The Politics of Defense Contracting: The Iron Triangle* (New York, NY: Council on Economic Priorities, 1981); on strategic and technology uncertainty, see Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca, NY: Cornell University Press, 1991), 185-220

defense acquisition render it uniquely resistant to overhaul.[65] Transaction costs must also include the staff officer effort to build and understand slides like Figure 4-5.[66]

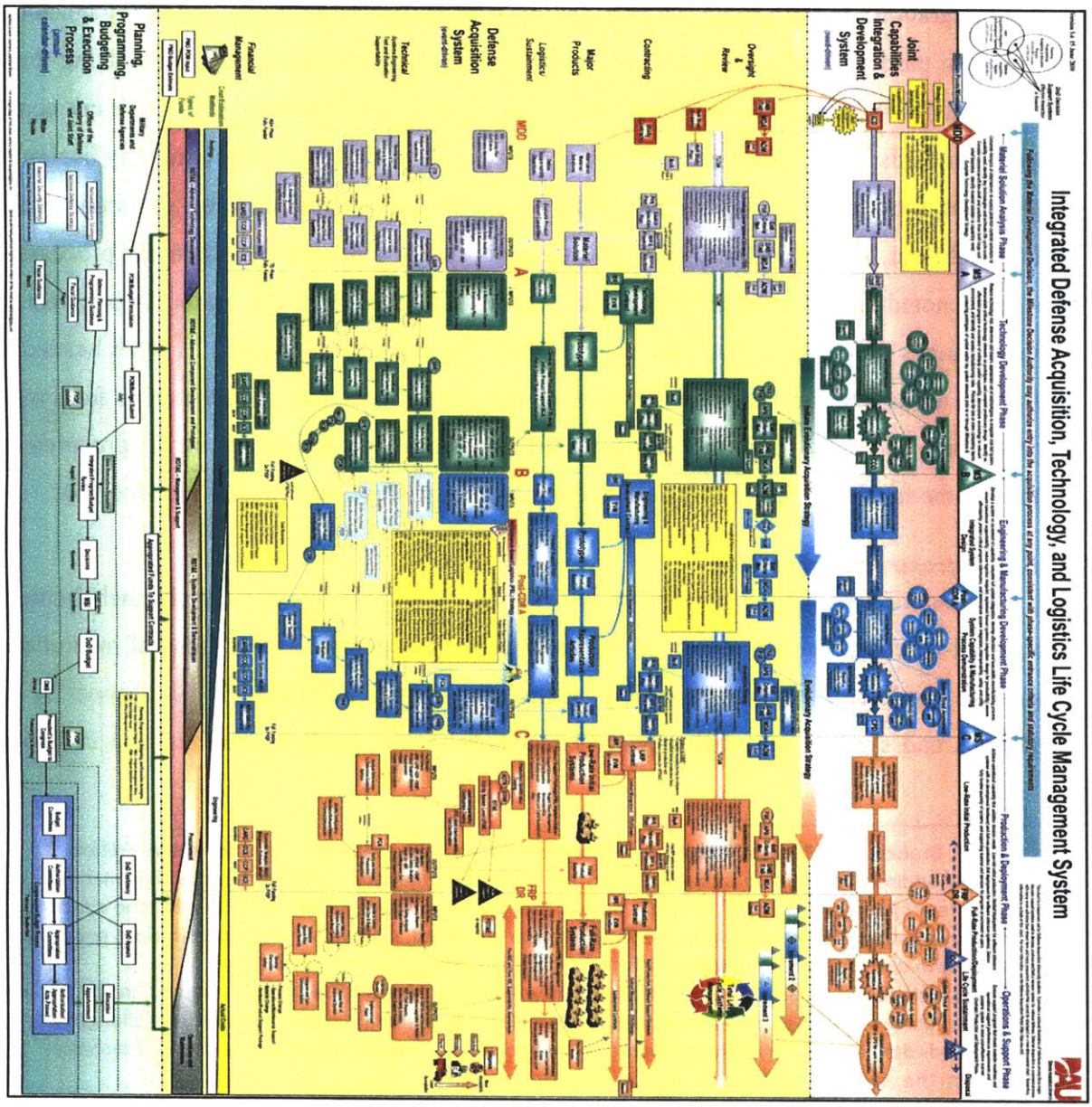


Figure 4-5: Complex transactions costs in defense technology procurement (DAU Chart).

---

[65] Thomas L. McNaugher, "Weapons Procurement: The Futility of Reform," in *America's Defense*, ed. Michael Mandelbaum (New York, NY: Holmes & Meier Publishers, 1989): 68-112; Alex Roland, *The Military-Industrial Complex* (American Historical Association, 2001); Wilbur D. Jones, *Arming the Eagle: A History of United States Weapons Acquisition Since 1775* (Fort Belvoir, VA: Defense Systems Management College Press, 1999)

[66] Defense Acquisition University, "Integrated Life Cycle Chart," 15 June 2010, https://ilc.dau.mil/pdfs/Front_Ver_54_June_15_2010_34x22.pdf

The pathologies of the defense industry affect software in spades. The vast number of states and non-linear interactions between abstract and arbitrary software components frustrates system integration.[67] The generative potential of modularity has its limits, for as organizations specialize in particular architectures and lose the knowledge that went into standardizing them, they get caught in a "modularity trap," unable to exploit new opportunities which cut across existing standards.[68] A 2000 Defense Science Board study found "software is rapidly becoming a significant, if not the most significant, portion of DOD acquisitions" and yet "programs lacked well thought-out, disciplined program management and/or software development processes." The study noted that almost all the major problems identified in six major Department of Defense studies on software acquisition since 1987 had not been corrected.[69] Such headaches tend not to attract the most talented software developers or most able IT technicians from more lucrative pay and less hassle in corporate firms. Gross inefficiencies in IT procurement compound the friction generated by normal defense industry and policymaker rent-seeking.

4.3.5.2 Infrastructural Lock-in

Economic transactions depend on institutions for durable information channels between actors. Set-up costs, learning costs, coordination costs, and actors' expectations of institutional persistence reinforce reliance on existing institutions. Actors rationally find it cheaper to use institutions and systems that they already know how to use, or that everyone else is already

---

[67] Frederick P. Brooks, *The Mythical Man Month: Essays on Software Engineering, 20th Anniversary Edition* (Reading, MA: Addison-Wesley Publishing Co, 1995); His whimsical summary is "Brooks' Law: Adding manpower to a late software project makes it later" (p. 232). Brooks' "tar pit" of software problems uncannily echo criticisms of government regulation: too little too late, over-budget, over-managed, plagued with communications problems, out of touch with users, difficult to update, difficult to maintain, disappointing, frustrating.

[68] Henry Chesbrough, "Towards a Dynamics of Modularity: A Cyclical Model of Technical Advance," in *The Business of Systems Integration*: 174-200. In a similar vein, David D. Clark describes (in conversation) the challenge of timing standards definition as "the two elephants of the apocalypse," caught between a ferment of technical exploration on the one hand and the lock in of market embrace on the other.

[69] Defense Science Board, *Report of the Defense Science Board Task Force on Defense Software* (November 2000), ES1-ES2, 3. Similarly, U.S. Government Accountability Office, "Stronger Management Practices Are Needed to Improve DOD's Software-Intensive Weapon Acquisitions," GAO-04-393 (March 2004), 1, finds that "DOD estimates that it spends about 40 percent of its Research, Development, Test, and Evaluation budget on software—$21 billion for fiscal year 2003. Furthermore, DOD and industry experience indicates that about $8 billion (40 percent) of that amount may be spent on reworking software because of quality-related issues....DOD did not have effective and consistent corporate or software processes for software acquisitions." See also on the deep problems in defense IT procurement through traditional acquisition channels, David C. Gompert, Charles L. Barry, and Alf A. Andreassen, "Extending the User's Reach: Responsive Networking for Integrated Military Operations," National Defense University, Center for Technology and National Security Policy, Defense and Technology Paper No. 24 (2006)

using, than to switch to new ones.[70] Because technology is so deeply intertwined with modern institutions, infrastructures develop in path-dependent fashion by the same logic (QUERTY keyboard and VHS videotapes are the classic examples).[71] Third-party software developers leverage the stability of software platforms like Microsoft *Office* to create new customizations and products which extend them. These third-parties become invested in the platform's persistence, and their new products and business processes dependent on them. Path dependent lock-in of software is not in and of itself a bad thing, for its stability lowers the costs of building sophisticated new functionality on a stable foundation.[72] Yet by the same logic, invisible coding gaffs and undocumented work-arounds become entrenched. "Angry orphans" demand continued support for outdated systems on which they depend.[73] Interdependent structure locks in legacy systems even when more efficient alternatives become available. Hence the despair often heard from RMA proponents that short-sighted organizations only apply IT incrementally to existing weapon platforms and doctrine rather than embrace its true "revolutionary" potential.[74]

4.3.5.3 Work-to-Rule Slowdown

Pervasive computerization can create an unintentional "work-to-rule" slowdown. When labor activists employ this protest strategy, employees do exactly and only what is explicitly described in corporate policy. They take all of their allotted breaks, follow every procedure to the letter, employ no work-arounds, and take no extra effort. Their punctilious obedience to corporate policy holds production hostage without the provocation of picketing or lock-outs. A

---

[70] Douglass C. North, "Institutions," *Journal of Economic Perspectives* vol. 5, no. 1 (1991): 97-112; Paul Pierson, "Increasing Returns, Path Dependence, and the Study of Politics," *American Political Science Review* vol. 94, no. 2 (2000): 251-267; Kenneth A. Shepsle, "Studying Institutions: Some Lessons from the Rational Choice Approach," *Journal of Theoretical Politics* vol. 1, no. 2 (1989): 131-147.

[71] Paul A. David, "Understanding the Economics of QWERTY: The Necessity of History," in *Economic History and the Modern Historian*, ed. W. Parker (London: Blackwell, 1986), 30-49; W. Brian Arthur, "Competing Technologies, Increasing Returns, and Lock-In by Historical Events," *Economic Journal* vol. 99, no. 394 (1989): 116-131. For an argument against technological lock-in in general and the famous QWERTY example in particular see S. J. Liebowitz and Stephen E. Margolis, "The Fable of the Keys," *Journal of Law and Economics* vol. 33, no. 1 (1990): 1-25.

[72] In biology, the lock-in of ancient genetic pathways and morphological structure is addressed as "deep homology" or "generative entrenchment." See Stephen J. Gould, *The Structure of Evolutionary Theory* (Cambridge, MA: Belknap Press, 2002); William C. Wimsatt, "Generative Entrenchment and the Developmental Systems Approach to Evolutionary Process," in *Cycles of Contingency: Developmental Systems and Evolution*, ed., Susan Oyama, Paul E. Griffiths, and Russell D. Gray (Cambridge: MIT Press, 2001): 219-238.

[73] Claudio Ciborra, "Imbrication of Representations: Risk and Digital Technologies," *Journal of Management Studies* vol. 43, no. 6 (2006): 1339–1356

[74] Elizabeth A. Stanley, "Evolutionary Technology in the Current Revolution in Military Affairs: The Army Tactical Command and Control System," US Army War College, Strategic Studies Institute, March 1998

work-to-rule strike quietly yet dramatically shows just how much production relies on labor's skillful, situated interpretation, discretion, and initiative—that is, on expedient adaptation.[75]

The creeping empowerment of those routine functions most amenable to automation introduces an insidious slowdown. Paul Attewell points out that "administrative overhead, far from being curtailed by the introduction of office automation and subsequent information technologies, has increased steadily across a broad range of industries."[76] Total organizations like the military regulate members' tactical training and readiness, security clearances, gear provision, travel, fitness, medical readiness, financial health, family situation, career progression, *etc.* All of these functions depend on clerical routines which apply to broad classes of uniform (literally) people and events. Tracking databases, online surveys and training, access-control cards, digital security policy and certificates, and web-based information portals all provide tools for expanding the reach of midlevel management. All of these different systems are subject to technical configuration and security regulation by zealous IT managers who control accounts, network access, application certification, and who can shut down services at the first sign of cyber-intrusion or "spillage" of classified information. Such systems generate quantified statistics about personnel and units delinquent in their bureaucratic obligations. Easy-to-measure statistics simplify performance evaluations, and discrepancies mobilize senior officers' ire over non-compliance with minor yet visible requirements. As the battlefield is a safer place for American soldiers now than it was for their forefathers, career signals then loom larger for personnel facing diminished existential threats. Officers find themselves legible in different databases and accountable to many systems beyond their control.

In a work-to-rule slowdown, the interests of bureaucratic principals are beholden to the interests of technical functionaries, both human and machine. Weber's iron cage becomes a silicon cage. The only reason that bureaucracies don't just seize up altogether is that employees undertake expedient adaptation to work around the Kafkaesque absurdity.

4.3.5.4 Conceptual Myopia

The lock-in of legacy systems and their administrative overhead may be frustrating and inefficient, but it is effectiveness rather than efficiency at stake in battlefield performance.

---

[75] Scott, *Seeing Like a State*, 310-311

[76] Paul Attewell, "Information Technology and the Productivity Paradox," in *Organizational Linkages: Understanding the Productivity Paradox*, ed. D. Harris (Washington, DC: National Academy Press, 1994): 13-53.

Administrative burdens can displace officers' attention from mission effectiveness; bureaucratic performance measures are clear and quantified while measures of battlefield effectiveness are ambiguous and confusing, so the former metrics of compliance capture attention. Yet an even more worrisome problem is that IT can help lock in worldviews.

Insulated militaries conduct the same types of operations repeatedly without being able to perceive the counterproductive side effects they generate. Units in the field report what they believe headquarters wants to know.[77] Headquarters aggregate performance metrics that demonstrate progress along their preferred performance vectors. As organizations develop data feeds and displays that support command and control of their most dangerous and most risky options, they see more opportunities to exercise them. The information system is insulating even though the organization might be quite connected to the environment in other ways, through its tactical patrols or bombing. For example, modern militaries regularly have trouble implementing the political dimension of counterinsurgency because they instead focus on the more tactically-tractable problem of hunting down insurgents for which they have ready intelligence, doctrine, and clear measures of performance, in lieu of measures of effectiveness.[78]

Many intelligence failures result from inabilities to share information as a result of mutual suspicion, which is rhetorically justified to protect sensitive sources, ignorance about other agencies' information sources, and simple technical incompatibility. In cases of surprise attack, intelligence insulation turns quickly into interference at the systemic level. Weak warnings or none at all emerged from Army and Navy inability to share their respective "Purple" decrypts of Japanese traffic prior to the raid on Pearl Harbor, or FBI and CIA reticence to coordinate terrorism data prior to 9/11. Costly data-management efforts are isolated within organizations tied down with red tape. As Roberta Wohlstetter famously describes warning failure, the signal gets lost in the noise.[79]

---

[77] Barry D. Watts, "Unreported History and Unit Effectiveness," *Journal of Strategic Studies* vol. 12, no. 1 (1989): 88-98

[78] Colin F. Jackson, "Defeat in Victory: Organizational Learning Dysfunction in Counterinsurgency," Ph.D. Dissertation, Massachusetts Institute of Technology, 2008.

[79] Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962); Richard K. Betts, *Surprise Attack: Lessons for Defense Planning* (Washington DC: Brookings Institute, 1982); Richard K. Betts, *Enemies of Intelligence: Knowledge and Power in American National Security* (Columbia University Press, 2007); Robert Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca NY:

4.3.5.5 The Grand Lamasery

Deleterious insulation is most likely when there is too much internal consensus in an environment which is structurally unstable. The most striking historical example is the stark contrast between the calm of World War I headquarters and the horror of trench combat. The extreme dissimilarity has given rise to a "lions led by donkeys" historiography and searing satire like the British television series *Blackadder Goes Forth*. J.F.C. Fuller disparaged General Headquarters (GHQ) as a "grand lamasery":

> The real weakness of GHQ did not lie in the character of any of these individuals, but in the lamaistic system which prevailed...[British Commanding General Douglas] Haig worked there like a mechanical monk...There was little or no contact with reality—with the circumstances which surrounded the cutting edge of the army. Hence time and again this edge was blunted, jagged or even broken.[80]

Historians have recently cast more sympathetic light on the administrative performance of the giant armies,[81] but still agree that "the continuing expansion of GHQ, combined with its well-established location, tended to isolate it from its front line units...and the result was a breakdown of trust between the Staff and those they directed and supplied."[82] After the Battle of Passchendaele—notorious for the mud which devoured tanks and infantry units without a trace—the British Chief of Staff suffered a nervous breakdown upon realizing that he had ordered men to advance through a sea of mud.[83] A 1959 paper by Harvard professor M.D. Feld observes:

> The function of command and the function of leadership, one devoted exclusively to planning and the other to execution, develop their peculiar mysteries. The problems of one remain remote to the other not merely because they are unwitnessed but also because in the context of the assigned task they are devoid of meaning. The fact that one organization is hierarchically superior to the other gives an invidious interpretation to this mutual incomprehensibility. Staff

---

Cornell University Press, 2010); Joshua Rovner and Austin Long, "The Perils of Shallow Theory: Intelligence Reform and the 9/11 Commission," *International Journal of Intelligence and Counterintelligence* vol. 18, no. 4 (2005): 609-637

[80] Quoted in Dan Todman, "The Grand Lamasery Revisited: General Headquarters on the Western Front, 1914-1918," in *Command and Control on the Western Front: The British Army's Experience 1914-18*, ed. Gary Sheffield and Dan Todman (Staplehurst, UK: Spellmount Publishers, 2004), 39.

[81] See, *inter alia*, the excellent volume by Sheffeld and Todman (note 80), and Ian Malcolm Brown, *British Logistics on the Western Front: 1914-1919* (Westport, CT: Praeger, 1998)

[82] Todman, "The Grand Lamasery Revisited," 58-59

[83] *Ibid.*, 59

> information eludes comprehension because it is esoteric; line information because it is trivial.[84]

Feld further argues that the radically different interpretations of Passchendaele—foolhardy tactical disaster versus strategic relief of French allies on the verge of mutiny and collapse—follow from the differences between line and staff information processing in "a situation in which battle was tactically impossible though strategically desirable...The deadlock enforced by barbed wire and automatic weapons brought about an almost complete disassociation of strategic and tactical thought...neither was in a position to guide the other. It was rather a matter of outright dominance, and the framework of organization gave staff the upper hand."[85] With too much internal consensus in a structurally unstable world, staff officers seem to work inside of a hermetically sealed bubble, unable to perceive or adapt to the turbulence of battlefield reality. Centers of calculation literally become "closed worlds."[86]

Table 4-5 summarizes hypotheses on about internal consensus and friction.

Table 4-5: Hypotheses on the effect of internal consensus on information friction (IC→IF)

Internal Consensus		Lowers Information Friction ↑	Raises Information Friction ↑
IC1.	Doctrinal preferences	Agreement on ends/means	Incompatible ends/means
IC2.	Number of actors	few, stable	Many, fluctuating
IC3.	Autonomy	"Unity of command"	Interdependence
IC4.	Division of labor	Defined, legitimate "lanes in the road"	Controversy over roles, functions, access to information
IC5.	Definition of protocols	Commensurable, comprehensive, impersonal, explicit, quantified	Fragmented, particular, idiosyncratic, tacit, qualitative
IC6.	Complexity management	Systems integration	Agency & transaction costs
IC7.	Semantic interoperability	Common ontology	"Stovepipes," fratricide, veracity bubbles
IC8.	Investment	Economies of scale	Rent-seeking, "iron triangle"
IC9.	Adjustment	Coordinated, deliberate	Lock-in, myopia, staff insulation
IC10.	Accountability	Auditing, depersonalized normative standards	Work-to-rule, risk-aversion

[84] M. D. Feld, "Information and Authority: The Structure of Military Organization," *American Sociological Review* vol. 24, no. 1 (1959), 16-18

[85] *Ibid.*, 21

[86] Paul N. Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America* (Cambridge, MA: MIT Press, 1996)

4.4 Expedient Adaptation in Human-Computer Interaction

The conditions of external stability and internal consensus are pretty austere. They are unlikely to hold up in war, which almost by definition is uncertain and controversial. Thus the third condition for lowering information friction is an organizational capacity to actively address it in the course of actual operations. Clausewitz often emphasizes the importance of adapting to circumstances rather than applying standard solutions: "War is not like a field of wheat, which, without regard to the individual stalk, may be mown more or less efficiently depending on the quality of the scythe; it is like a stand of mature trees in which the axe has to be used judiciously according to the characteristics and development of each individual trunk."[87] Members of large organizations often interpret the spirit of corporate policy generously and discretely tailor their interpretation to local circumstances.[88] Likewise, personnel often bypass cumbersome IT infrastructure and cobble together expedient prototypes for their local data management needs. "We are all cognitive bricoleurs," as Edwin Hutchins describes distributed cognition, "opportunistic assemblers of functional systems composed of internal and external structures."[89] Expedient adaptation is improvisation with the information resources at hand by personnel who understand both the supply-side possibilities of the technology and the demand-side requirements of the mission.

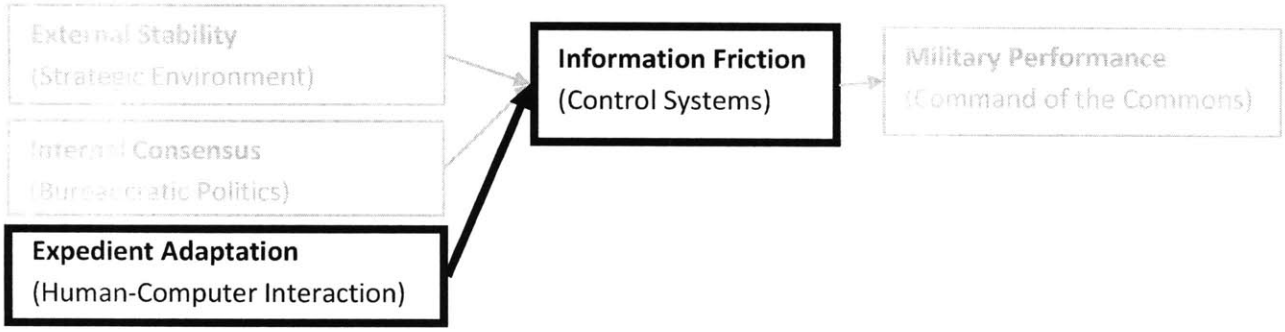


Figure 4-6: Causal relation between expedient adaptation and information friction

4.4.1 User Innovation

Eric Von Hippel shows that in a wide range of industries, individuals create novel products and processes without seeking patents because they personally benefit from using the

---

[87] Clausewitz, *On War*, 153

[88] Michael Lipsky, *Street-Level Bureaucracy: Dilemmas of the Individual in Public Services* (New York: Russell Sage Foundation, 1980)

[89] Edwin Hutchins, *Cognition in the Wild* (Cambridge, MA: MIT Press, 1995), 172.

invention rather than selling it.[90] Manufacturers often do not perceive the emerging market trends which "lead users" experience because situated knowledge of their niche is hard to communicate. Lead users find it cheaper to make up a prototype with their particular skills and discretionary resources. For example, an emergency medical technician (EMT) and avid mountain biker attached surgical tubing and an IV bag to his cycling jersey to create the first prototype of what would become the popular *Camelbak* line of hydration systems. Lead users often freely reveal their inventions to peers, who then use and further improve them, thereby generating self-reinforcing user innovation communities. The dynamics of "user innovation communities" have also been described as "open-source design" or "peer-production." Extreme sports, scientific instrumentation, and software communities all feature prodigious levels of user innovation.[91]

Likewise in war, field expedient adaptation of weapons and tactics is as old as the Trojan Horse.[92] After the landings at Normandy, the Allied advance slowed to a crawl in the dense hedgerows which afforded German ambushes. American G.I.s fashioned hedgerow cutters for Sherman tanks out of German beach obstacles, and infantrymen, tankers, and engineers pioneered novel cooperative tactics to finally enable tactical advance.[93] The "improvised explosive device" (IED) has become the iconic weapon of choice of America's adversaries in recent wars, and servicemen have responded with all sorts of improvised countermeasures to defeat the triggering or detonation of IEDs.[94] Not surprisingly, soldiers have also taken to improvising with IT. As one reporter observed during the 2003 invasion of Iraq:

---

[90] Eric Von Hippel, *Democratizing Innovation* (Cambridge, MA: MIT Press, 2005); Eric Von Hippel, *The Sources of Innovation* (New York, NY: Oxford University Press, 1988)

[91] Nelly Oudshoorn and Trevor Pinch, *How Users Matter: the Co-Construction of Users and Technology* (Cambridge MA: MIT Press, 2003); Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (New Haven, CT: Yale University Press, 2007)

[92] Accounts of battlefield expedients are a staple of most combat histories, but there are few thematic treatments. See James Jay Carafano, *GI Ingenuity: Improvisation, Technology, and Winning World War II* (Mechanicsburg, PA: Stackpole Books, 2006); Center of Military History, *Improvisations During the Russian Campaign* (Washington DC: United States Army, 1986); John H. Hay, *Tactical and Materiel Innovations, Vietnam Studies* (Washington, D.C.: Department of the Army, 1974)

[93] Michael D. Doubler, *Closing With the Enemy: How GIs Fought the War in Europe, 1944-1945* (University Press of Kansas, 1995), 43-48. Doubler's study is full of bottom-up expedient adaptations.

[94] See the four-part multimedia series in the *Washington Post* by Rick Atkinson, "Left of Boom: The Fight Against Roadside Bombs," 30 September through 3 October 2007, http://www.washingtonpost.com/wp-srv/world/specials/leftofboom

> I tracked the network from the generals' plasma screens at Central Command to the forward nodes on the battlefields in Iraq. What I discovered was something entirely different from the shiny picture of techno-supremacy touted by the proponents of the Rumsfeld doctrine. I found an unsung corps of geeks improvising as they went, cobbling together a remarkable system from a hodgepodge of military-built networking technology, off-the-shelf gear, miles of Ethernet cable, and commercial software. And during two weeks in the war zone, I never heard anyone mention the revolution in military affairs.[95]

The 1st Marine Division's 2003 lessons learned report from Iraq observed that "data on [the official shared database] was often untrustworthy" and "other track management systems did not appear to function at all." Noting "a number of technical and management issues with the [official Common Tactical Picture]," the report describes the dawning recognition of insulation friction, "the enemy did not conform to our expectation of a conventional line and block organization for combat." Expedient adaptation to the rescue: "the Division created its own methodology of disseminating [custom] overlays every 2-3 hours with the current assessed enemy picture. The Division deliberately chose a periodic quality-controlled product over real-time erroneous information. This process also was flexible enough to handle the non-standard nature of the enemy." This report item concluded that "Track management [designed by official contractors] seems to work well to track enemy airplanes or submarines, but is not flexible enough to reflect ground organization for combat at tactically usable levels."[96]

Cases of such ersatz IT development can be found throughout recent military history. The first digital aid for naval anti-air warfare was a product of a savvy user/developer group with support from senior officers.[97] Even after the Navy established formal electronic system procurement offices, members of the USS *Eisenhower* carrier battle group cobbled together a tactical decision-aid system during a large exercise in 1981, with some of the actual software written by sailors. JOTS (originally the "Jerry O. Tuttle System" after the battle group commander and later "Joint Operational Tactical System") replaced a costly Navy system that had been under development for a decade. Admiral Tuttle later commanded the Naval Space and Electronic Warfare Command (SPAWAR), completing JOTS's transition from informal

---

[95] Joshua Davis, "If We Run Out of Batteries, This War Is Screwed," *Wired* (June 2003)
[96] 1st Marine Division, "Operation Iraqi Freedom (OIF): Lessons Learned," May 2003, 11-12
[97] David L. Boslaugh, *When Computers Went to Sea: The Digitization of the United States Navy* (Los Alamitos, CA: IEEE Computer Society Press, 2003)

experiment to program of record.[98] In the 1980s Army geospatial software procurement suffered recurring delays and cost increases, while informal prototypes emerged through the West Point computer science department and became popular with users.[99] In a more recent and thoroughly typical example, a U.S. artillery training team found itself training the Afghan National Army with Soviet doctrine and equipment. NATO protractors (6400 mils) were incompatible with Soviet protractors (6000 mils), map references were inverted, and powder charges were measured on different scales, among other problems. Their solution was a Microsoft *Access* database that could translate between NATO and Soviet settings. U.S. personnel tinkered with the interface until it was easy enough for the Afghans to use.[100] It seems like almost every unit has its own pet *Access* database to pull together all the odds and ends that don't fit into officially-sanctioned data management schemes.[101]

User innovation with IT is endemic in the U.S. military; however, expedient adaptation is not only the *fact* of user innovation, but also the *relief* of information friction thereby. Sometimes informal local adjustments can be counterproductive, as examples of interference throughout these pages suggest. Expedient adaptation, therefore, is a certain mindful competence among, and institutional encouragement of, the user community to guide this natural adaptive ferment in a productive direction.[102] The conditions detailed below—open technology, low barriers to technical expertise in forward locations, and institutional support for user innovation—improve the odds that bottom-up adjustments will lower information friction. These conditions show that bottom-up organizational adaptation is somewhat broader than the

---

[98] Norman Friedman, *Seapower and Space: From the Dawn of the Missile Age to Net-Centric Warfare* (Anapolis, MD: Naval Institute Press, 2000), 217-22, 354n

[99] Donna J. Peuquet and Todd Bacastow, "Organizational Issues in the Development of Geographical Information Systems: A Case Study of U.S. Army Topographic Information Automation," *International Journal of Geographical Information Science* vol. 5, no. 3 (1991): 303 - 319

[100] Daryl L. Fullerton, "Back to the Basics: Training Army Artillerymen to Grow Afghan National Army Artillerymen," *Air Land Sea Bulletin* vol. 2008, no. 3 (2008): 4-7

[101] Stories of military user innovation with IT are rife in professional journals, either penned by the inventor himself or a commander lauding some genius which just happened to appear in his unit. See for example, Michael A. Raymond, "COP: Fusing Battalion Intelligence," *Fires Bulletin* (January-February 2008): 29

[102] Ciborra, *Labyrinths of Information*, describes opportunistic mission-focused use of local circumstances in waging war or managing corporate information systems.

phrase "user innovation" might imply. Expedient adaptation is often messy and surely not a panacea, but it's better than epistemic dysfunction.[103]

4.4.2 Interpretive Flexibility

Technology that maximizes possibilities for creative recombination is a permissive condition for expedient adaptation. Ronald Kline and Trevor Pinch describe the openness of technology to end-user adaptation as "interpretive flexibility." They describe how American farmers converted the Ford Model T into a general-purpose engine to run washing machines, pumps, and machine tools.[104]

While many types of technology offer some interpretive flexibility, IT is unprecedented in its affordance of user innovation. All innovation stems from the recombination of existing processes and devices into new functionality.[105] This is nowhere as true as with IT, because it is literally built out of layers of modular components. From the emergence of programmable calculators to application-building toolkits for *Facebook* and *iPhone*, the history of the IT industry has been one of increasingly powerful design opportunities devolving to the individual user.[106] An increase in flexibility doesn't automatically mean more efficiency, just as consumer appliances did not reduce the domestic workload on housewives.[107] Furthermore, generative opportunities can be dangerous in the wrong hands, like giving power tools to children or weapons to criminals.[108] They can be exploited as readily by state power as by the techno-libertarian.[109] Yet whether used for good or ill, the generative potential of IT is incontrovertible.

---

[103] On the low-level ferment of technological and tactical adaptation in recent counterinsurgencies see: James A. Russell, "Innovation in War: Counterinsurgency Operations in Anbar and Ninewa Provinces, Iraq, 2005-2007," *Journal of Strategic Studies* vol. 33, no. 4 (2010): 595 – 624; Theo Farrell, "Improving in War: Military Adaptation and the British in Helmand Province, Afghanistan, 2006-2009," *Journal of Strategic Studies* vol. 33, no. 4 (2010): 567 - 594

[104] Ronald Kline and Trevor Pinch, "Users As Agents of Technological Change: the Social Construction of the Automobile in the Rural United States," *Technology and Culture* vol. 37, no. 4 (1996): 763-795. On the continuing end-user modification of automobiles in the hot rod community see David N. Lucsko, *The Business of Speed: The Hot Rod Industry in America, 1915-1990* (Baltimore, MD: The Johns Hopkins University Press, 2008)

[105] W. Brian Arthur, *The Nature of Technology: What It Is and How It Evolves* (New York, NY: Free Press, 2009)

[106] Martin Campbell-Kelly, *From Airline Reservations to Sonic the Hedgehog: A History of the Software Industry* (Cambridge, MA: MIT Press, 2004)

[107] Ruth Schwartz Cowan, *More Work for Mother: The Ironies of Household Technology from the Open Hearth to the Microwave* (New York, NY: Basic Books, 1983)

[108] Zittrain, "Generative Internet"

[109] Most IT futurism contains some utopian version of techno-democracy; see the collection in Adam Brate, *Technomanifestos* (New York: Texere, 2002). By contrast, states have maintained a lot of control of IT: Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (New York, NY: Oxford

Whether or not interpretive flexibility also lowers information friction depends on how responsibly it's exploited.[110]

4.4.2.1 Extensible Interfaces and Toolkits

Many applications feature macro-writing toolkits or scripting support like the *Visual Basic for Applications* programming environment in the Microsoft *Office* suite. Application programming interfaces (APIs) and software development kits (SDKs) expose the functionality of compiled applications to third party developers. These enable existing functionality to be incorporated into customized programs. The more software components, file formats, and configuration options that are exposed in a human-readable format, the greater the generative potential. Documentation and online help further facilitates extensibility. For example, databases that output to a *FalconView* or *Google Earth* format can display their data on a map, which extends the functionality of both applications. Toolkits lower the costs of user innovation by providing collections of parts and processes that users can recombine.[111]

Much commercial software has explicitly embraced configurability and third-party development because it enables products to be expanded into new markets by consumers themselves. A whole industry of third-party Microsoft *Office* developers help to cement the dependence of countless firms on the dominant software suite and create continued demand for new improvements from the Redmond giant. Much of this extensibility has been introduced into military organizations inadvertently as they buy commercial operating systems and productivity software. While an unplanned boon for military expedient adaptation, it also consternates network administrators worried about "mobile code" and other security externalities of extensibility.

4.4.2.2 Proprietary Software and Open Source

Licensed software inhibits expedient adaptation by limiting diffusion only to users who are able to obtain a license. Licensing may further specify or prohibit what types of modification are allowed. The debate between proponents of freely-available "open source" and proprietary

---

University Press, 2006); Shanthi Kalathil and Taylor C. Boas, *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule* (Washington DC: Carnegie Endowment for International Peace, 2003)

[110] This project is geeky enough already that I might as well quote from *Spiderman (Amazing Fantasy #15)*: "with great power there must also come—great responsibility!"

[111] Stefan Thomke and Eric Von Hippel, "Customers As Innovators: A New Way to Create Value," *Harvard Business Review* vol. 80, no. 4 (2002): 74-81

software can reach frenzy of religious proportions,[112] but the relative quality of the two approaches remains an open question. Open code certainly does provide opportunities for people to learn about how it works and to make changes. Examples and often assistance from other open-source developers are available to the user-developer online. However, proprietary code is often better supported with documentation and dedicated technical support, and it provides a stable set of components to recombine into new uses.

4.4.2.3 Discretionary Resources

Slack resources—discretionary spending, spare parts, extra time, or reserve capacity—are the raw materials that personnel use to put together prototypes and experiment with new processes for unexpected circumstances. Simple poverty might limit discretionary resources, but more often the managerial pursuit of efficiency and "just in time" spares provision cuts out slack. When every part and man-hour must be accounted for, then it becomes more difficult to justify consumption for the sake of experimentation that might fail. Slack is indeed inefficient, but for precisely that reason it enables invention of things that fall outside of efficiency criteria.

A lot of redundant informational residua linger about on file servers indefinitely, much like so-called "junk DNA" on the human genome which appears to never be expressed. Yet this structure can be opportunistically incorporated into new functions. Martha Feldman describes how analytical reports produced by a U.S. government agency were very rarely read by their ostensible consumers. Nevertheless, she found that the byproducts of producing the reports were actually more important than the reports themselves: the research process generated data, forced conversations, and built knowledge the analysts used to meet *ad hoc* queries.[113] A disturbing example of repurposing an existing implementation is a system of punch cards developed in 1930s France to aid the mobilization of conscripts, which was later co-opted by the Nazi occupation to identify Jews.[114] Expedient adaptation can clearly be put to evil purposes in the wrong hands.

---

[112] For the popular case for open-source see Eric S. Raymond, *The Cathedral and the Bazaar, Rev. Ed.* (Cambridge, MA: O'Reilly, 2001). For a more nuanced economic argument see Josh Lerner and Jean Tirole, "Some Simple Economics of Open Source," *Journal of Industrial Economics* vol. 50, no. 2 (2002): 197-234

[113] Martha S. Feldman, *Order without Design: Information Production and Policy Making* (Stanford University Press, 1989)

[114] Lars Heide, "Monitoring People: Dynamics and Hazards of Record Management in France, 1935-1944," *Technology and Culture* vol. 45, no. 1 (2004): 80-101

Gene Rochlin's cautionary analysis of commercial, financial, and military computerization focuses on the ossification of adaptive capability.[115] His overriding critique of organizational IT is that managerial enthusiasm for large-scale systems reduces slack and thus builds in potentials for catastrophic failures:

> What is lost in many cases is not just variety, and specific human skills, but the capacity to nurture, enhance, and expand them through the messy process of direct, trial and error learning. Computerization and automation are also wonderful promoters of the icon of technical efficiency, as opposed to the duplicative and often haphazard maintenance of sufficient extra resources to control or mitigate the effects of human mistakes. Of particular concern is the degree to which what is destroyed or discarded in the relentless pursuit of technical and operational efficiency is not waste or slop, but "slack," the human and material buffering capacity that allows organizations and social systems to absorb unpredicted, and often unpredictable, shocks.[116]

The openness of IT architectures to further design and the availability of slack resources are permissive conditions for expedient adaptation. For those qualities to lower information friction, however, the potential must be mated to technical expertise and operational context.

4.4.3 Low Barriers to Technical Expertise

Knowledge about how technology works and what people actually do with it tends to be embodied in tacit practice and changeable circumstances. As discussed in Chapter 3, situated knowledge is "sticky" on both the supply and demand sides.[117] Expedient adaptation is improved (and information friction lowered) when both types of information can be brought together or "unstuck."

4.4.3.1 Forward Location of Technical Expertise

Traditional weapons acquisition programs depend on formally articulated and officially validated requirements which separate engineers from forward users with many layers of bureaucratic interface. While justified on enterprise integration considerations, this process can also insulate technical investments from operational communities whenever situated knowledge

---

[115] Gene I. Rochlin, *Trapped in the Net: The Unanticipated Consequences of Computerization* (Princeton, NJ: Princeton University Press, 1997); also see Thomas K. Landauer, *The Trouble With Computers: Usefulness, Usability, and Productivity* (Cambridge, MA: MIT Press, 1996).

[116] *Ibid.*, 213.

[117] Eric Von Hippel, ""Sticky Information" and the Locus of Problem Solving: Implications for Innovation," *Management Science* vol. 40, no. 4 (1994): 429-439

is particularly nuanced and/or subject to rapid change. Busy users deployed around the world tend not to articulate long-term requirements as they focus on a short-term mission. Thus staff officers located echelons above and at least a tour away from operational experience draft requirements. The "Planning, Programming, Budgeting, and Execution" process for U.S. system development is outpaced by rapid change in the commercial IT industry and the emergence of new operational needs. The integration of hundreds of engineers and managers spread across programs, subcontractors, and geographical locations makes for perpetual *PowerPoint* presentations, meetings, emails, Gantt charts, and configuration control documents. Such barriers between IT supply and demand increase information friction.

Conversely, when engineers and operators can be brought together, then they share information about possibilities and needs more easily. The further forward this union of supply and demand expertise, the more likely prototypes will emerge that will be both technically sound and operationally tailored. Engineers will be excited to discover sweet problems and find it rewarding to see people using their solutions, and operators will be excited to receive help in reducing their information friction without having to work through a recalcitrant bureaucracy. They adapt prototypes to emergent needs and test them with actual data with all its unexpected permutations (never captured in too-clean test data). Because not all of the relevant information resides in the brains of users, but also in IT affordances and social interactions, it is better to move technical expertise forward into this context than to drag operational expertise to the rear. Nevertheless, any such transit between the loci of expertise will improve expedient adaptation.

4.4.3.2 Boundary-Spanning Figures

At the extreme, the engineer and operator might be one and the same person. Individuals who understand both how information works and what information means will be most successful in adapting systems to lower friction. War fighting and engineering are both fulltime jobs, yet some individuals do have enough experience and credibility in multiple domains to serve as a bridge between them. Boundary-spanning individuals open up information and resource channels among the communities who need to work together.[118] A classic example is Henry Tizard, who was a British fighter pilot in World War One and a scientist in "the establishment" who moved easily between Air Ministry positions and academia. As will be

[118] Michael L. Tushman and Thomas J. Scanlan, "Boundary Spanning Individuals: Their Role in Information Transfer and Their Antecedents," *Academy of Management Journal* vol. 24, no. 2 (1981): 289-305

discussed in chapter 8, Tizard played a key role in linking radar scientists to the Royal Air Force. Organizations that recruit and retain boundary spanners will enhance expedient adaptation.

4.4.3.3 Technical Literacy

At the risk of stating the obvious, personnel who have training and experience with IT are better suited to debugging it. They will be more receptive to and more likely to seek out interaction with engineers. Their learning times for new applications will be shorter. They will be more attentive to pitfalls in data management. They will be better able to search for and make sense of online data.

The non-obvious caveat is that digital literacy does not necessarily entail competency in computer science. The maturation of software tends to hide a lot of its internal workings within an increasingly robust "user illusion." Application-building "wizards" help motivated but technically naïve users assemble shoddy databases with serious scaling and interoperability issues. The technical literacy at stake here is familiarity with the general leakiness of all abstractions and some experience in the art of computer science and knowledge management to cope with it. Gaining such literacy without losing operational focus is a major recruitment and training challenge. Cross-trained operators are expensive.

Personnel in the U.S. all-volunteer force tend to have a higher degree of technical literacy relative to other militaries. The U.S. has an advanced industrial recruiting pool with an increasing proportion of recruits who are "digital natives." The military offers generous in-house vocational and college educational incentives for retention. Operations are steadily more knowledge intensive so more personnel tend to gain experience with IT in exercises and combat. This general literacy explains much of the rambunctious ferment of IT improvisation in operational U.S. organizations. Yet because the osmosis of skilled personnel into forward situations where they might prototype innovative solutions is still a rather *ad hoc* process, many actual improvisations tend to be quite *ad hoc* in technical quality as well.

4.4.3.4 User Communities

To the degree that personnel can share their particular information and expertise with one another, either online or by circulating through different worksites, then expedient adaptation will be enhanced. Lead users freely reveal inventions and share them with peers, who further improve the invention as they tailor it to their own needs. User groups share tips, advice, and

assist debugging one another's information systems. Isolated or uncooperative users, by contrast, are more likely to increase information friction because they receive no technical advice and less mindful of how their modifications might affect other users of the information system.

4.4.3.5 Practical Ethnography

In the presence of high information friction, people constantly have to switch their attention from content to format. Since operational information systems usually feature many informal interactions and Rube Goldberg mashups, people have to find out what their own organizations are actually doing if they want to have any hope of debugging them. Ulrike Schultze, reflecting on her participant-observer study of computer system administrators, intelligence analysts, and librarians in an IT-intensive firm, found that knowledge workers actually performed a lot of the same activities that she did as an ethnographer: discovering and articulating tacit interactions, monitoring social relationships, and translating work activity in one domain for an audience from another.[119]

Michael Kometer describes this spontaneous ethnography in a U.S. Combined Air Operations Center (CAOC): "The [targeting] cell was interpreting and sharing information—often resolving ambiguous messages and determining who should see what and in what channel. Moreover, it was managing team dynamics—cueing others, teaching and learning roles, figuring out where they were in the process, and establishing trust."[120] Thus practitioners had to take their eyes off simply passing information content and attend to the format of systems and their group dynamics. Sometimes information processes were so confusing as to require deliberate investigatory effort: "To collect and process the information, [the chief of assessment] had to gain personal contact with the operations. He had seven to nine contractor analysts working for him, but instead of turning them loose to analyze the information, he had to send them to gather the data. He sent them to the different cells within the CAOC, including two or three on the combat operations floor at any given time, to figure out how the various cells turned data into information and which of it could be useful for their assessments."[121] The resort to amateur ethnographic research raises the question of what professionally-trained researchers might have

---

[119] Ulrike Schultze, "A Confessional Account of an Ethnography about Knowledge Work," *MIS Quarterly* vol. 24, no. 1 (2000): 3-41

[120] Michael W. Kometer, *Command in Air War: Centralized Versus Decentralized Control of Combat Airpower* (Maxwell Air Force Base, AL: Air University Press, 2007), 174

[121] *Ibid.*, 176

been able to find, but the fact that it emerges spontaneously in the course of knowledge work is interesting and important.

To the degree that personnel take the time to survey technical and social dimensions of their own information systems, the more likely they will be able to identify and articulate the sources of information friction. The first step to designing an effective runtime solution is to understand the sociotechnical problem. By contrast, ethnographically naïve adaptations of IT, which are undertaken without curiosity or regard for their broader context of use, will tend to exacerbate information friction.[122]

4.4.4 Institutional Support for User Innovation

While informal user innovation occurs almost spontaneously in military units, the development of staying power, the provision of legitimate tool kits, and nurturance of a robust user community all need the consent and support of formal bureaucratic authority. Expedient adaptive *capacity* is therefore itself something of a design time feature. If internal consensus includes provision for expedient adaptation in its scheme for enterprise integration, then it is more likely that spontaneous user innovation will lower information friction rather than raise it. Expedient adaptive capacity is an architecture which expects and facilitates its own change.[123] Clausewitz never said that militaries shouldn't make war plans; he just recommends that long-term plans should also include the cultivation of officers with "genius" to deal with the upset of operational plans upon contact with the enemy. Information friction needs wartime debuggers.

An exemplary case of military user innovation is *FalconView*, the *de facto* standard for geospatial information management in U.S. mission planning and intelligence communities.[124] During the PC boom of the 1980s, Air Force fighter pilots wrote flight-planning software using inexpensive PCs, and shared it freely with their comrades. These expedients anticipated and often suggested features that were later incorporated into official systems. Personnel explored areas of functionality that the official programs said would be too hard or too expensive, notably with planning tools that interoperated across service communities. Again and again, official

---

[122] Diana E. Forsythe, *Studying Those Who Study Us: An Anthropologist in the World of Artificial Intelligence* (Stanford, CA: Stanford University Press, 2001), 132-162

[123] David D. Clark, Karen Sollins, John Wroclawski and Ted Faber, "Addressing Reality: An Architectural Response to Real-World Demands on the Evolving Internet," ACM SIGCOMM Workshops, Karlsruhe, Germany, August 2003

[124] A more detailed case study of *FalconView* can be found in Jon R. Lindsay, "War Upon the Map: User Innovation in American Military Software," *Technology and Culture* vol. 51, no. 3 (2010): 619-651

procurement programs ran into extraordinary difficulty and expense as formal requirements, federal budget cycles, sharply defined jurisdictions, classification, and acquisitions red tape separated users from engineers. By contrast, *FalconView* outsourced the definition of requirements and the prototyping of novel functionality to the users themselves. Personnel used toolkits like *FalconView*'s developer interfaces and Microsoft's *Visual Basic* to produce working applications for air wars like Kosovo and irregular conflicts like Afghanistan.[125]

Successful user innovation didn't happen all by itself, however. Traditional acquisition and network management regimes viewed military user development activity as unsustainable and illegitimate. *FalconView* supporters thus had to turn organizational barriers into opportunities in order to get funding and build institutional support. They leveraged organizational schisms—such as between the Air Force and Air National Guard or between aviation and ground communities—and they exploited policy loopholes. Despite the stark surface contrast between user enthusiasm for *FalconView* and user antipathy for official systems, there was a more complicated interdependence between official and unofficial software systems. In a series of mutual accommodations, some of the same officers managed both types of programs; both types shared common software components and map data; the formal programs looked to the renegades for requirements and assistance covering shortfalls; *FalconView* could enjoy the luxury of ignoring some high-end computational or mission-sensitive functions; and *FalconView* management eventually took on a more bureaucratic character in order to comply with certification and testing policy. The literature on user innovation often depicts a spontaneous self-organizing process, but in fact it requires institutional management to provide recombinable tools and to solve integration problems. The requirement for an institutional platform for decentralized innovation is even more critical with the personnel rotation and lethal outcomes associated with military organizations. *FalconView*'s community shaped technological and institutional structure in order to support an innovation.[126]

---

[125] It is ironic that Microsoft products enable so much user innovation in the military given that the firm is so vilified in open-source discourse. While few civilian engineers would choose to write an application in Visual Basic, normal software development packages (to enable users to code C++ or Java projects) are prohibited on most working military networks.

[126] John Law, "Technology and Heterogeneous Engineering: The Case of Portuguese Expansion," in Bijker, Hughes, and Pinch, *Social Construction of Technological Systems*, 111-134

For every story of users developing innovative solutions and building institutional support, however, there are countless more of inventions that either wither away when Dr. Frankenstein transfers or are crushed when they cross into an adverse regulatory jurisdiction. While expedient adaptation is the only emollient that can relieve information friction once war is underway, decentralized adaptation inherently risks creating interference friction for the larger system. The weakening of internal consensus, or devolution of initiative to local actors, becomes a resource for adaptation to the particular turbulence of the operational problem. But selfish optimization of local data management can also exacerbate negative externalities and coordination failure. Sober systems integrators rightly worry that amateur software is insecure, unreliable, personality-dependent, and difficult to scale up and maintain. Such technocrats also tend to pardon the bloated inefficiency and rent-seeking associated with their own insulated projects, which often prompt expedient adaptation in the first place.

4.4.5 Chaos in the CAOC

Michael Kometer's study of Air Force command and control during the four major U.S. air campaigns from 1991 to 2003 documents many instances of local design activity in Combined Air Operations Centers (CAOC).[127] Pervasive bottom up innovation was necessary to operate, but all of this local activity, even though undertaken with the best intentions to solve local problems, sometimes created further integration problems.

In Operation Desert Storm (Iraq, 1991), planners "used markers, pens, and pencils to mark the target locations on charts," and they then input information into five different systems without a common database. There was no "picture of the way all the missions fit together to accomplish the objectives" and so "information did not come over data link in a systematic way, but rather from the informal links [the planner] was able to assemble from the sources within his reach."[128] Over the next decade automated planning systems began to provide alternatives to markers and maps, but only to introduce interoperability problems.

During Operation Allied Force (Kosovo, 1999), planning data was "produced in a message format that was readable only by special parsers. As the war dragged on, planners

---

[127] Kometer, *Command in Air War,* especially Ch. 6, "The Center of the CAOS," 153-184

[128] *Ibid.*, 155-157. Tremendous interoperability challenges and informal manual workarounds in this same environment are also described in Alexander S. Cochran, ed., *Gulf War Air Power Survey, Volume 1, Planning and Command and Control* (Washington, DC: Government Printing Office, 1993)

developed their own Microsoft *Excel* spreadsheets, *Word* documents, and other tools to perform their own functions." Because these tools were often incompatible and not all planners worked in the same buildings or on the same classified networks, the air commander's staff "took the information, converted much of it to [Microsoft] *Access* format for manipulation, and created *PowerPoint* briefings...This enormous task was the digital equivalent of collecting everyone's yellow stickies to create napkin-sketches of the progress of the entire air campaign."[129]

System interoperability improved somewhat for Operation Enduring Freedom (Afghanistan, 2001), but with a high tempo of operations and many new intelligence sensors to integrate, informal Microsoft work-arounds remained critical. "Planners said that [Master Air Attack Plan] briefing slides represented their view of the world...It was much easier to understand than the [Air Tasking Order], which was sent out in a confusing message format. They looked at the...briefing to see the planned flow of aircraft and an application called *FalconView* to see where the aircraft were in real time." Informal activity spanned incompatible systems using not only IT systems, but also by physically walking around printouts: "Those in the [targeting] Cell coordinated with others in the CAOC by walking around to get signatures on a routing spreadsheet, e-mailing, or telephoning. Since the Judge Advocate General was in another part of the building and the point mensurators [who calculate coordinates for precision weapons] were in another building with the [intelligence] division, they walked around a lot."[130]

Operation Iraqi Freedom (Iraq, 2003) stressed air planners further by requiring coordination with a fast-paced land invasion. Despite prior air-ground coordination at operational headquarters, many problems emerged in the interface between Air Force targeting and Army fire support systems, which required the improvisation of several intermediate data stores (usually Microsoft *Office* files), many of them populated manually. For example, "the Army worked out a way to send all [Air Support Requests] as interdiction requests and then send code in the remarks section that would indicate the mission was other than interdiction," which meant personnel were exploiting the flexibility of free-text fields to convey information that system design had not considered. "There were well over 100 colonels in the CAOC, and each seemed to have another problem like [the 'other than interdiction' request] to solve. The result

---

[129] *Ibid.* 161-162
[130] *Ibid.*, 166-167

was a lot of customized information formats."[131] Unfortunately, all these rampant data management problems and their expedient solutions created confusion in the aggregate. "It is no wonder when [the air commander] asked [the deputy chief of strategy] for results on day two of the war, [he] could not even tell [the commander] what the air component had done, not to mention how it had gone."[132]

The low-level initiative required to work through information friction can inadvertently exacerbate not only interference, but also insulation. Personnel were "able to create innovative solutions to several problems they had passing data internally and among organizations in the CAOC." However, "autonomy had a price—it made it more difficult for the Strategy Division to determine the results in the aggregate...In fact, the better the centers get at intervening in real-time missions, the harder it is for them to determine what is going on in the aggregate."[133] As a result, "Army officers who worked for the CAOC...pointed out that the inability of the air component to determine and communicate the effects of airpower was the biggest source of friction between the air and land components."[134] The *ad hoc* workarounds of existing systems and all the effort to integrate workarounds canalized the organization into a myopic focus on improving time-critical targeting rather than creating comprehensive representations to connect strategic objectives to tactical activity.

In Kometer's account of four air campaigns, the importance of expedient adaptation in working through endemic information friction is apparent. Systems were rarely used as planned, and tremendous human effort was required to build up technical and process scaffolding for them to work at all. To the extent that personnel were able to develop any sort of understanding of targets and threats in the world, it was because they actively reconfigured the information systems to which they had local access. The low adaptation costs of their IT allowed personnel to adapt their local environments effectively as long as their task remained locally stable, with well-defined communication interfaces across organizational boundaries. Yet as local

---

[131] *Ibid.*, 176. For a confirming account of the information friction in this specific case of air-ground system interface, see Thomas L. Kelly and John P. Andreasen, "Joint Fires: A BCD Perspective in Operation Iraqi Freedom," *Field Artillery* November-December 2003: 20-25

[132] *Ibid.*, 177

[133] Michael W. Kometer, *Command in Air War: Centralized Versus Decentralized Control of Combat Airpower* (Maxwell Air Force Base, AL: Air University Press, 2007), 177, 180.

[134] *Ibid.*, 175

rationalization made it feasible to exchange data, the challenges of sharing data across boundaries became acute.

Table 4-6 summarizes hypotheses about how expedient adaptation affects friction.

Table 4-6: Hypotheses on the effect of expedient adaptation on information friction (EA→IF)

Expedient Adaptation	Lowers Information Friction ↑	Raises Information Friction ↑
EA1. Extensibility	Configurable interface, toolkits	Inflexible interface, locked code
EA2. Licensing	Open source	Proprietary
EA3. Discretionary resources	Spare time/labor/money, access to affordable commercial material	Little slack, all resources accountable
EA4. Location of technical expertise	Forward with operational users	Barriers between engineers and users
EA5. Novel designs	Informal prototyping	Formal requirements
EA6. Boundary-spanning figures	Access and credibility across disciplinary boundaries	Only formalized interaction across boundaries
EA7. Technical literacy	Education, experience, enthusiasm	Variable quality, technophobic
EA8. User community	Collegial exchange of ideas & prototypes	Rigid formal coordination, isolated/uncooperative users
EA9. Practical ethnography	Deliberate investigation of actual representational practices	Adaptations ignore practical context of IT usage
EA10. User innovation support	Enable & reward initiative, experimentation, communities	Suppress or ignore user innovation
EA11. Organizational retention	Select and support promising user inventions	Enforce conformity to officially-sanctioned tools
EA12. Externalities	Lead users mindful of their positive & negative externalities	Myopic focus on private improvements

4.5 Complex Missions and Technologies Create Information Friction

The reader may have noticed that some of the causes of information friction covered in this chapter are mutually inconsistent. Internal consensus and expedient adaptation especially appear to be at odds. Indeed, the enterprise integration condition of low information friction involves coordinated rational management, whereas expedient adaptation is an organic self-organized activity that works around and sometimes in spite of formal control. Enterprise integration is good for large-scale reliability while expedient adaptation is good for adaptation to unexpected situations. Unfortunately, the former risks generating the insulation variety of high information friction, while the latter risks causing interference. The ferment of user invention

and the institutional control of technical standards often stand in contradiction.[135] Harvey Sapolsky describes the impasse:

> Organizations that are decentralized and diverse in terms of their skill base are more likely to generate ideas for innovation but are exactly the kinds of organizations that have trouble adopting new ideas. Diversity leads to counter offers, the proposal of innovations that favor your team or sub-unit against rivals and conflict over opportunities, the battle for the choice jurisdiction, and thus to difficulty in gaining agreement on the path to take. More centralized, less diverse organizations...generate fewer ideas, but can more easily make decisions.[136]

In the context of military command and control, Martin van Creveld similarly observes that "greater certainty at the top (more reserves, superior control) is only bought at the expense of less certainty at the bottom." The problem is thus less about eliminating uncertainty than about "a different distribution of uncertainty among the various ranks of the hierarchy."[137]

Complex organizations try to square the circle by managing different layers of their information system with different modes of control. The modular abstraction of IT architectures readily enables the partition of command. Yet the same architecture provides many opportunities for personnel to intervene for better or for worse in the attempt to coordinate internal and external structure. Advances in IT tend to complicate an organization's balancing of the risks of too much order and too much chaos in each layer and interconnections across them.[138] The organization's formal and informal attempts to address the fundamental tensions in their information systems usually add more layers, modules, symbols, distinctions, network policies, normative constraints, working groups, coordination meetings, training programs, *etc.* Over time, information friction acts like a complexity ratchet for a control-seeking organization.[139]

---

[135] James Q. Wilson, "Innovation in Organization: Notes towards a Theory," in *Approaches to Organizational Design*, ed. James D. Thompson (University of Pittsburgh Press, 1966): 194-218

[136] Harvey M. Sapolsky, "On the Theory of Military Innovation," *Breakthroughs* vol. 9, no. 1 (2000): 35-39

[137] Van Creveld, *Command in War*, 274. "From Plato to NATO, the history of command in war consists essentially of an endless quest for certainty," 264.

[138] Jeffrey K. Liker, Carol J. Haddad and Jennifer Karlin, "Perspectives on Technology and Work Organization," *Annual Review of Sociology* vol. 25 (1999), 593, concludes that "technology influences complex social networks and acts sometimes as an integrative force and other times as a disintegrative force that separates people."

[139] James R. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge, MA: Harvard University Press, 1986), argues that increasing industrial throughput, reliability, and

As control systems mature they enable the military to perform ambitious missions where they will be more likely to experience information friction. More actors doing more things, in larger areas and shorter time spans, with a proliferating set of protocols to coordinate their behavior, cannot but help to exacerbate problems of both external stability and internal consensus. Battles will tend to be fought in politically-fraught contested zones. The adoption of autonomous weapons and sensors moves humans rearward in articulation and perception cascades. As a result, the integration phase of the control cycle becomes more complex and labor-intensive. The endogenous growth of information friction abets the shift, described in Chapter 1, of much of the military workforce into knowledge work and out of physical combat. It is beyond my scope to develop this dynamic mechanism much further in this dissertation.[140]

The subsequent chapters will show information friction in action in empirical cases of organizations at war. The ethnographic chapters describe my experience in Iraq with a special operations unit. The Battle of Britain chapter shows information friction in a radically different strategic, historical, cultural, and technological context. These cases both have very different values on the causes of (low) information friction—*external stability* of the battlefield, *internal consensus* about technical protocols, and *expedient adaptation* of IT by operational users—and as a result very different patterns of enterprise integration, interference, and insulation.

---

predictability of production from the 1880s to the present leads to increasing returns on control, which increases demand for control, including the need to control the controls. Chris C. Demchak, *Military Organizations, Complex Machines: Modernization in the U.S. Armed Services* (Ithaca, NY: Cornell University Press, 1991), highlights "rogue outcomes" in the unexpected management and maintenance requirements of advanced weapon systems. Michael Tomasello, *The Cultural Origins of Human Cognition* (Cambridge, MA: Harvard University Press, 2000), describes the co-evolution of human cognitive capacity and cultural capacities in similar terms.

[140] I offer a diagram and some tentative hypotheses in an appendix, Endogenous Growth of Information Friction.

Chapter 5: Special Operations in al-Anbar

> "If we had a modern state, we wouldn't have to rely on the rule of tribes, but until then a little bit of evil is better than more." –Sheikh Hamid al-Hais[1]

5.1 Participant-Observation in Iraq

In this and the next two chapters I will use the framework developed in the previous two chapters to describe information processes within a U.S. special operations task force (SOTF, pronounced "sō'tif") in Iraq in 2007-2008. This case is based on my experience with the SOTF as a uniformed military officer, mobilized from the naval reserve while in graduate school at MIT to active duty with the Office of Naval Intelligence. In my capacity as Officer in Charge of a Tactical Intelligence Support Team attached to the SOTF, I was responsible for personnel in a variety of analytical and intelligence collection roles. I also served as the "Non-Lethal Effects Officer" on the SOTF staff where I coordinated tribal engagement, civil affairs, and psychological operations in western Iraq. In the normal course of my duties I traveled to various operating sites along the Euphrates River and worked across all SOTF staff sections, so I was able to get a good feeling for the organization's information practices.

This chapter provides background on the war in Iraq's Anbar province, where the SOTF was deployed, as well as the peculiar culture of U.S. Special Operations Forces (SOF). It is organized in terms of the three causes of information friction discussed in the previous chapter. To summarize their values in this case up front, *external stability* was low because the highly localized and dynamic battlefield was full of furtive insurgents and tribal actors with fickle loyalties. *Internal consensus* was low overall because of the complicated menagerie of counterinsurgent actors from different services, government agencies, and coalition partners; however, within the SOTF itself it was higher because of its operational autonomy from conventional forces and strong doctrinal preferences for commando raids ("direct action"). *Expedient adaptation* was ambiguous because ubiquitous Microsoft technology combined with a special operations ethos of improvisation promoted expedient adaptation, but nevertheless, technical expertise was very uneven and so adaptations carried negative externalities. These conditions together lead us to expect high information friction in both its interference and

[1] Anthony Shadid, "Iraq Election Highlights Ascendancy of Tribes," *Washington Post*, 25 January 2009, A1

insulation variants, which the following two chapters will assess in turn. Before launching into the substantive material, I address some methodological challenges.

5.1.1 "This is where the magic happens"

Because this case relies on a somewhat unusual research strategy with an unusual subculture, a narrative introduction to the field site might be helpful. In a famous passage of *On War*, Clausewitz walks the novice onto the battlefield. From "the slope where the commanding general is stationed with his large staff" he takes us through progressively mounting danger and fear up to "the firing line, where the infantry endures the hammering for hours."[2] The journey to our headquarters in Iraq happens in reverse. Compared to popular images of fast-roping commandos and daring firefights, this journey to the heart of modern special operations will seem anticlimactic.

Our scene begins in a darkened helicopter speeding through the night, the cabin stuffed with a dozen sailors, Marines, civilian reporters, Bangladeshi catering contractors, and pallets of supplies. Without warning the pilot takes aggressive evasive maneuvers, flares eject into the night, and door gunners fire several bursts at unseen assailants. We soon pass over the danger from the town below and arrive over a darkened landing zone "inside the wire," within the well-protected perimeter of the Forward Operating Base. Once on the ground, eerie green cabin lights turn on and a crewmember waves us out. We gather up our kit and shuffle through the rumbling rotor wash toward an orange-lit gap in the concrete blast walls. In a squat wooden building, transient passengers sit around eating pork chops in Styrofoam containers and a young Marine checks our ID cards. A van is waiting to drive away from the airfield, down a dirt road past some smiling Ugandan guards who stand near trash-barrel fires with their AK-47s. Once on a paved road, we turn on the headlights and drive past artillery pits, tank parks, convoys of humvees. The surreality fades into humdrum normalcy as we pass road signs, traffic police, and groups of well-kempt Marines walking between the chow hall and the well-stocked commissary.

On the outskirts of the base we approach another compound surrounded by blast walls, sand-filled gabions and a heavy steel gate which looks like a set from a *Mad Max* movie. Through the gate is an odd collection of military and civilian vehicles. Guys in shorts with shaggy hair and mustaches saunter about with the casual bearing of California surfers. They're

[2] Clausewitz, *On War*, 113

working out, working on weapons, and playing video games that are far more violent than anything they'll actually experience on this deployment. We clamber out of the van and enter a complex of Alaskan Shelter tents.

Once inside the well-lit air-conditioned space, we peel off our body armor and stow our weapons in cubby holes beside an impressive pantry of snack food. In one wing of the tent is the operations center, where several rows of bored-looking civilians and sailors in brown t-shirts sit in front of laptops. On the front wall some projectors display Predator drone video of a suburban neighborhood, where it appears nothing interesting is happening, and also a spreadsheet listing upcoming missions. In the next tent, apart from the racks of weapons and the rough plywood and canvas workmanship, there is really nothing out of the ordinary. People sit behind desks covered with computer monitors, stacks of papers, family mementos and humorous kitsch, chatting on the phone and to one another. The next building over has a conference room with comfortable chairs and a video-teleconferencing screen. This "battle staff" works more or less in an expeditionary office building, "just living the dream," doing all the mundane things that people do in offices everywhere.

On this short journey we've crossed over several boundaries, each revealing important characteristics of this world. Our movement from "outside the wire" with its dangers of sudden ambush by an unseen enemy to the relative safety of the base highlights how the administration of violence requires the construction of robust administrative infrastructure. Our movement from the regimented realm of conventional forces to the more casual world of special operations highlights the existence of different military subcultures, rife with potential for misunderstanding as well as exchange between them. Our movement from the virile warrior culture of "operators" to the desk-bound life of "staff bitches" highlights the way martial culture marginalizes information work, even though it is increasingly ubiquitous and essential in the conduct of modern war.[3] The more storied activity of special operations depends on sprawling information

[3] The U.S. military has a rich pejorative vocabulary for describing support and staff personnel, much of it developed self-deprecatingly by the REMFs (rear echelon...) themselves. A comic series called "BOB on the FOB," created by Sgt. A. J. Merrifield and originally published in the 101st Airborne Division's *Band of Brothers* magazine, features a cast of characters such as the FOBbit (who remains forever inside the wire because he always has one more email or PowerPoint to work on), TOCroach (who covets all the coffee and sticky-buns in the headquarters), Geardo (who obtains the latest tactical gadgets without ever using them in combat), Storyfeller (who drones on about life back in the day), and the Good Idea Fairy (who feeds upon the confusion created by frivolous change). "BOB on

infrastructure behind the scenes. This study will explore the role of information and technology in movements across all these boundaries: external stability, internal consensus, and human-computer interaction.

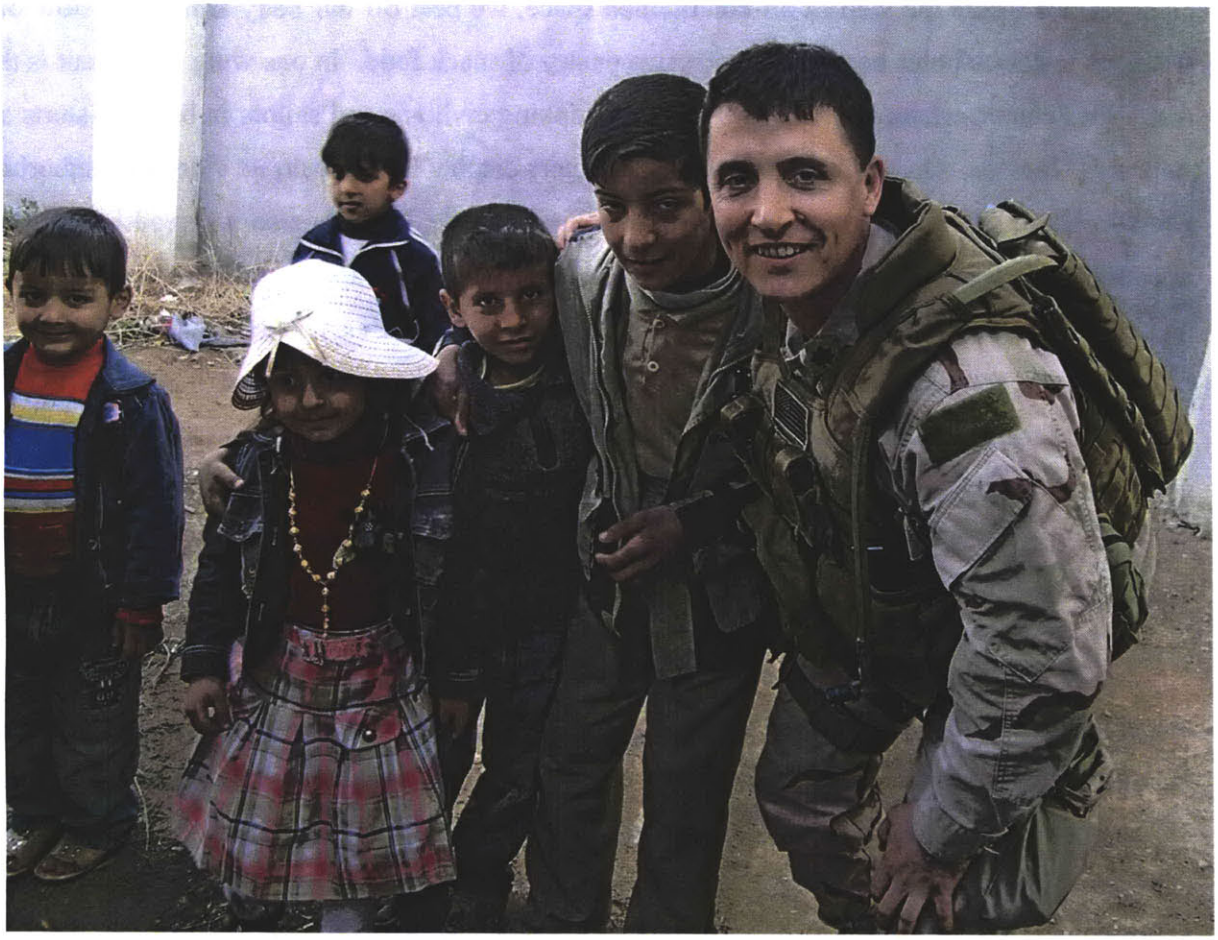


Figure 5-1: Author near Fallujah (Author's photo)

5.1.2 Active Duty

In traditional ethnography the researcher is an outsider entering into an alien culture to observe and articulate their life world.[4] By contrast, I was already something of an insider in

---

the FOB" comics are posted widely around bases in Iraq, self-consciously highlighting the absurdities of modern staff life in the spirit of Joseph Heller.

[4] See Chapter 1 for discussions of ethnography in general. This chapter discusses considerations particular to my site. I particularly found useful: Michael H. Agar, *The Professional Stranger: An Informal Introduction to Ethnography, 2nd Edition* (Elsevier Academic Press, 1996); Robert M. Emerson, Rachel I. Fretz and Linda L. Shaw, *Writing Ethnographic Fieldnotes* (Chicago, IL: University of Chicago Press, 1995); Diana E. Forsythe, *Studying Those*

this organization. I had served with the Naval Special Warfare community on active duty prior to graduate school. Thus I was already familiar with SOF culture, and I happened to already be acquainted with some of the key SOTF leaders. This eased my entrance into and acceptance by the community.[5]

Throughout the mobilization and deployment, my top priority was the performance of my military duties. Observation of information practices with intent to articulate them for this study was of necessity a passive concern. I was thus a participant first and an observer second: quite deliberately, I "went native." In addition to substantive concerns about the battlefield, officers also must worry a lot about the technology and processes they use to perceive and control the battlefield: they have to worry about what information means as well as how information works. Therefore, when I discussed information processes in depth with colleagues, it was a natural part of the work environment to do so, and it would have occurred in the absence of any research agenda. Being a knowledge worker involves paying attention to many of the same questions an ethnographer of knowledge work cares about.[6] My raw empirical material emerged as a by-product of natural interactions in the field, with my attention primed by prior theoretical study.

At the same time, I was open about my secondary civilian identity as a student of military information systems and my interest in using the deployment to Iraq as a case study. I found that my fellow sailors were extremely supportive and encouraging of this effort. When I told them I was writing a dissertation about the unintended consequences of computers in the military, they often laughed and told me I should definitely use the deployment as a case study. And so I have.

My fieldwork is an instance of what anthropologists call "studying up" institutions with power and influence in one's *own* culture; *i.e.*, studying the "colonizers" rather than the

---

Who Study Us: An Anthropologist in the World of Artificial Intelligence (Stanford, CA: Stanford University Press, 2001).

[5] John Van Maanen, *Tales of the Field: On Writing Ethnography* (Chicago, IL: University of Chicago Press, 1988) calls this first person idiom a "confessional" style which calls to attention the interactions between the field worker and the study environment—including the personal motivation for the study and the logistics of access—in order to provide insight into the advantages and limitations of the work as well as to emphasize that ethnography is an interpretive endeavor. The substantive portions of this ethnography assume what Van Maanen calls a "realist" style, describing the study phenomena as objectively as possible with minimal mention of the field worker's involvement. The brief preceding section on the helicopter flight is the only "impressionistic" style in this dissertation.

[6] Ulrike Schultze, "A Confessional Account of an Ethnography about Knowledge Work," *MIS Quarterly* vol. 24, no. 1 (2000): 3-41

"colonized."[7] Researchers in such situations can be employees of the organizations they study, subject to confidentiality agreements, and have employers who take an interest in how they will be portrayed. All of these considerations apply here in spades. Whereas ethnography generally eschews the passing of judgment on the practices of the study group, trying instead to describe them on their own terms, by contrast "studying up" often takes a more critical view by focusing on the exercise of power. My case is preoccupied with information pathologies that lead to military blunders, with an eye toward trying to lessen their frequency or severity. Comparable ethnographies in security organizations include fieldwork with police organizations as a police officer and research in working military or law enforcement settings where the fieldworker is a civilian but subject to austere constraints.[8]

5.1.3 Fieldnotes

My status as an officer in a military unit in a combat zone precluded the employment of standard ethnographic methods like on-site interviews or video recording of discourse and interactions. In order to protect myself, the mission, and classified information, I deliberately chose to refrain from documenting my experience—over and above the many notebooks I filled up in the daily course of staff work—until after demobilization. One methodology textbook states that "every hour spent observing requires an additional hour to write up."[9] With workdays already lasting sixteen hours or more every day, month after month, there just wasn't enough time in the day for that, and I didn't want to take time away from the military mission for extracurricular field notes. Jotting notes about detailed interactions would have taken me away from work that other people depended upon for dangerous decisions; it also would have interrupted natural interactions with colleagues. Field workers always face some suspicion from

---

[7] Laura Nader, "Up the Anthropologist: Perspectives Gained from Studying Up," in *Reinventing Anthropology*, ed. Dell H. Hymes (New York, NY, Pantheon Books, 1972): 284-311; Diana E. Forsythe, "Ethics and Politics of Studying Up in Technoscience," *Anthropology of Work Review*, vol. 20: 6-11

[8] See, *inter alia*, Peter K. Manning and John Van Maanen, ed., *Policing: A View From the Street* (New York, NY: Random House, 1978); Peter Moskos, *Cop in the Hood: My Year Policing Baltimore's Eastern District* (Princeton, NJ: Princeton University Press, 2008); Carolyn Nordstrom and Antonius C.G.M. Robbins, *Fieldwork under Fire* (University of California Press, 1995); Peter. B. Kraska, "Enjoying Militarism: Political/Personal Dilemmas in Studying U.S. Police Paramilitary Units," In *Ethnography At the Edge: Crime, Deviance, and Field Research*, ed. Jeff Ferrell and Mark S. Hamm (Boston, MA: Northeastern University Press, 1998), 88-110; Karl E. Weick and Karlene H. Roberts, "Collective Mind in Organizations: Heedful Interrelating on Flight Decks," *Administrative Science Quarterly* vol. 38, no. 3 (1993): 357-81

[9] Emerson, *et al*, *Writing Ethnographic Fieldnotes*, 39.

group members about note taking, but how much more within an access-controlled environment with strong in-group dynamics like special operations?

5.1.4 Classified Information

Abstinence from dedicated field notes also provided a firebreak between my daily classified-information working environment and the unclassified ethnography. I did sacrifice the sort of rich detail about interactions that distinguishes much ethnographic writing—who said what to whom with which gesture in what situation—so anything I wrote later would, unavoidably, be less fresh and more interpreted. I felt, however, that this trade off was worth it in order to be able to say *something* about this unique environment rather than nothing at all.

I am under legal obligation to protect the classified information to which I was exposed in the field. Given that ongoing U.S. operations still use protected sources and methods that put lives at stake, there is a moral obligation as well. This is a more severe manifestation of something all field workers must deal with in protecting the confidentiality of their informants. Researchers in corporate firms are analogous because they sign legal non-disclosure agreements to protect proprietary or private information. Confidentiality can be protected by using pseudonyms, ideal-type depictions of representational media, and avoiding information which identifies persons, methods, or events that aren't already in the public domain.

My overarching approach to the problem of classified information is to focus on recurring patterns of human-computer interaction rather than the content of specific events, reports, or sources and methods. Ethnography is a method for accessing unarticulated and culturally-situated phenomena. Bureaucratic information control policy, by contrast, clearly articulates which types of data are classified. A lot of the phenomena I am interested in are thus not classified because they are tacit features of social practice. This manuscript is subject to review by a government publication review board to ensure no inadvertent disclosure of classified information. Such a review does not affect the interpretations which are my own; furthermore, my interpretation of IT usage and staffwork is the primary contribution of this work, not any lurid details of special operations, which have already been retold in countless commando memoirs. There is already a great deal of information about intelligence and special operations in the public domain, so I make use of open source material to supplement my own observations. In the end, my account may not be as detailed as methodology textbooks

recommend, but it is still more comprehensive than any other account of everyday information practices in a modern operational environment.

5.1.5 Ethical Concerns

My commitment to participation over observation while mobilized should alleviate potential ethical concerns.[10] Since I did not ask anyone to engage in any interaction for the purposes of research that they weren't doing anyway in the normal course of combat operations, there is little risk that my field research could be construed as adversely affecting participants.[11] Since I am protecting classified information and omitting all references to specific people and events, there is little risk of research results negatively affecting specific individuals. My "field notes" are working staff notes and personal *ex post facto* recollections. No intrusive research was performed, and all private particulars are protected. My civilian identity as a graduate student was public knowledge among the study group. Lastly, government pre-publication review provides institutional consent with respect to the protection of sensitive information.

In contrast with traditional field research, this is more of a theoretically-informed reflection on my personal experience in an official capacity in Iraq.[12] If a social scientist who happens to be a military reservist is mobilized to active duty and then later writes about his experience, this is a totally different category from a civilian anthropologist working within or employed as an anthropologist by the military.[13] American military culture, furthermore,

---

[10] On related ethical challenges of field work with police or criminal cultures, see Jeff Ferrell and Mark S. Hamm, *Ethnography At the Edge: Crime, Deviance, and Field Research* (Boston, MA: Northeastern University Press, 1998)

[11] I am talking here about the process of observing altering behavior or psychology in some detrimental way. Whether or not other military personnel agree with my interpretations is a different matter. This ethnography does take a critical stance toward special operations culture, to which some members of the organization may take exception in the name of keeping controversies in house. Pretentions of ethical or classified information protection should not be used as a political excuse to censor criticism.

[12] Leon Anderson, "Analytic Autoethnography," *Journal of Contemporary Ethnography* vol. 35, no. 4 (2006): 373-395

[13] The American Anthropological Association (AAA) has vigorously protested the Army's "Human Terrain System," which involves hiring and deploying teams of anthropologists and soldiers to survey indigenous culture in support of counterinsurgency operations. For a description of HTS see Jacob Kipp, Lester Grau, Karl Prinslow and Don Smith, "The Human Terrain System: A CORDS For the 21st Century," *Military Review* (September-October 2006). For a thoughtful assessment of the program by an anthropologist—emphasizing how *American* military culture gets in the way of studying *local* culture—see David B. Edwards, "Counterinsurgency As a Cultural System," *Small Wars Journal* (27 December 2010), Http://smallwarsjournal.com/blog/journal/docs-temp/630-edwards.pdf. The AAA argues that HTS puts at risk both field workers (who can't be distinguished from military or intelligence personnel) and indigenous people (who may be subject to violence as a result of field work); see the AAA statement at http://www.aaanet.org/_cs_upload/pdf/4085_1.pdf. This debate has deep roots in the history of anthropology, which abetted colonial encroachment and domination of indigenous peoples by (1) providing

encourages officers to reflect on their wartime experience. In this respect the present study is like other practitioner reflections, but simply more grounded in a body of theoretical scholarship than most. Unclassified professional journals and war college papers are filled with first-person accounts that are critical in a spirit of reforming military institutions. Likewise, my criticism not only doesn't harm U.S. personnel, it potentially helps them by articulating important phenomena that can improve their performance of information-intensive military operations. Operational, intelligence, management, and acquisitions personnel need to appreciate information friction in order to devise reforms to better deal with it.

5.1.6 Theory Development and Writing

After I demobilized in the summer of 2008, I went through my notebooks and fleshed out my still-recent recollections regarding information processes. Instead of exhaustively defining variables and causal mechanisms prior to the deployment, I had first acquainted myself with general theoretical problems of representation and human-computer interaction in the sociology of technology literature. This primed my attention to theoretically salient phenomena while I was immersed in the field. Afterward, through careful reflection on and refinement of field notes against a background of prior sensitization to theoretical concepts, I teased out operative concepts, distinctions, and processes which structured representational practice at the SOTF. I refined information friction theory into specific concepts and hypotheses through an iterative process of comparing my theory against my progressively refined field notes. Observed data and theoretical insights emerged in a recursive deductive-inductive process. The substantive ethnography which follows is the result.[14]

---

intelligence about them and (2) promoting myths of racial essentialism. The controversy was reenergized during the Vietnam War as the US government employed anthropologists to support village pacification. What the AAA appears to ignore in the case of Iraq and Afghanistan, however, is that in a counterinsurgency soldiers will invariably become "amateur ethnographers" as they interact with local cultures to win "hearts and minds." Tragically, both soldiers and indigenous people pay the price for amateurish mistakes that could be avoided through more nuanced understanding of the culture in which, unfortunately, the war will be waged. The AAA conflates *jus ad bellum* with *jus in bello* concerns by taking an absolute position against abetting war at all while ignoring opportunities to improve its conduct—and lessen its human cost—once a particular war is underway. The concern for the politicization of anthropologists during war is itself a rather politicized position against war in general.

[14] Barney G. Glaser and Anselm Strauss, *Discovery of Grounded Theory: Strategies for Qualitative Research* (Chicago, IL: Aldine Publishing Co., 1967); Agar, *The Professional Stranger.*

5.2 External Instability of the Irregular Battlefield

The first condition for reliable information systems is the stability of the information problem, which means that features of the world must be knowable in principle. By contrast, messy battlefields, barriers to the creation and transmission of records, and agile enemies increase information friction. The SOTF operated in a complex and dynamic counterinsurgency environment with low external stability.

5.2.1 War in Anbar, 2003-2008

Iraq's Anbar province (Figure 5-2) is the largest province in Iraq and one of the most desolate. It is about the size of Arkansas, spanning the deserts west of Baghdad to the Syrian, Jordanian, and Saudi borders. U.S. forces during the study period (2007-8) divided Anbar into three administrative areas of operation: the western suburbs of Baghdad through Fallujah to the major logistics hub at Taqaddum airfield near Habbaniyah; the broad area around the provincial capital of Ramadi; and the western desert communities from Hit through the large reservoir at Haditha to Qaim on the Syrian border. Most of Anbar's 1.2 million inhabitants live in towns along the Western Euphrates River Valley (WERV), the dominant geographical feature. The vast deserts north and south of the WERV are largely inhospitable, constituting more of an exile than a refuge for insurgents. The WERV is a longstanding historical corridor for licit and illicit trade between the Levant and Baghdad, and after 2003 it became a channel for foreign fighters and weapons.

In contrast to Iraq's overall diverse ethnic and religious makeup, the Anbari population is almost exclusively Sunni Arab. Many of Saddam Hussein's Baath Party, Republican Guard, and intelligence service elite hailed from Anbar, which is the reason why the province became the locus of nationalist rebellion against the American occupation. At provincial as well as national levels, the influence of tribal authority, which is based around traditional patriarchal leadership rather than municipal laws, varies inversely with the influence of urban government.[15] One Marine general officer was fond of observing that in Anbar, "the tribes are not the government, but the government is of the tribes."

---

[15] Hosham Dawood, "The Stateization of the Tribe and the Tribalization of the State: The Case of Iraq," in *Tribes and Power: Nationalism and Ethnicity in the Middle East*, ed. Faleh Jabar and Hosham Dawood (London: Saqi Books, 2003); Amatzia Baram, "Neo-Tribalism in Iraq: Saddam Husayn's Tribal Policies 1991-1996," *Journal of Middle Eastern Studies* vol. 29, no. 1 (1997): 29-56; Lin Todd, *Iraq Tribal Study–al-Anbar Governorate: The Albu Fahd Tribe, the Albu Mahal Tribe and the Albu Issa Tribe*, Global Resources Group, Department of Defense, 2006

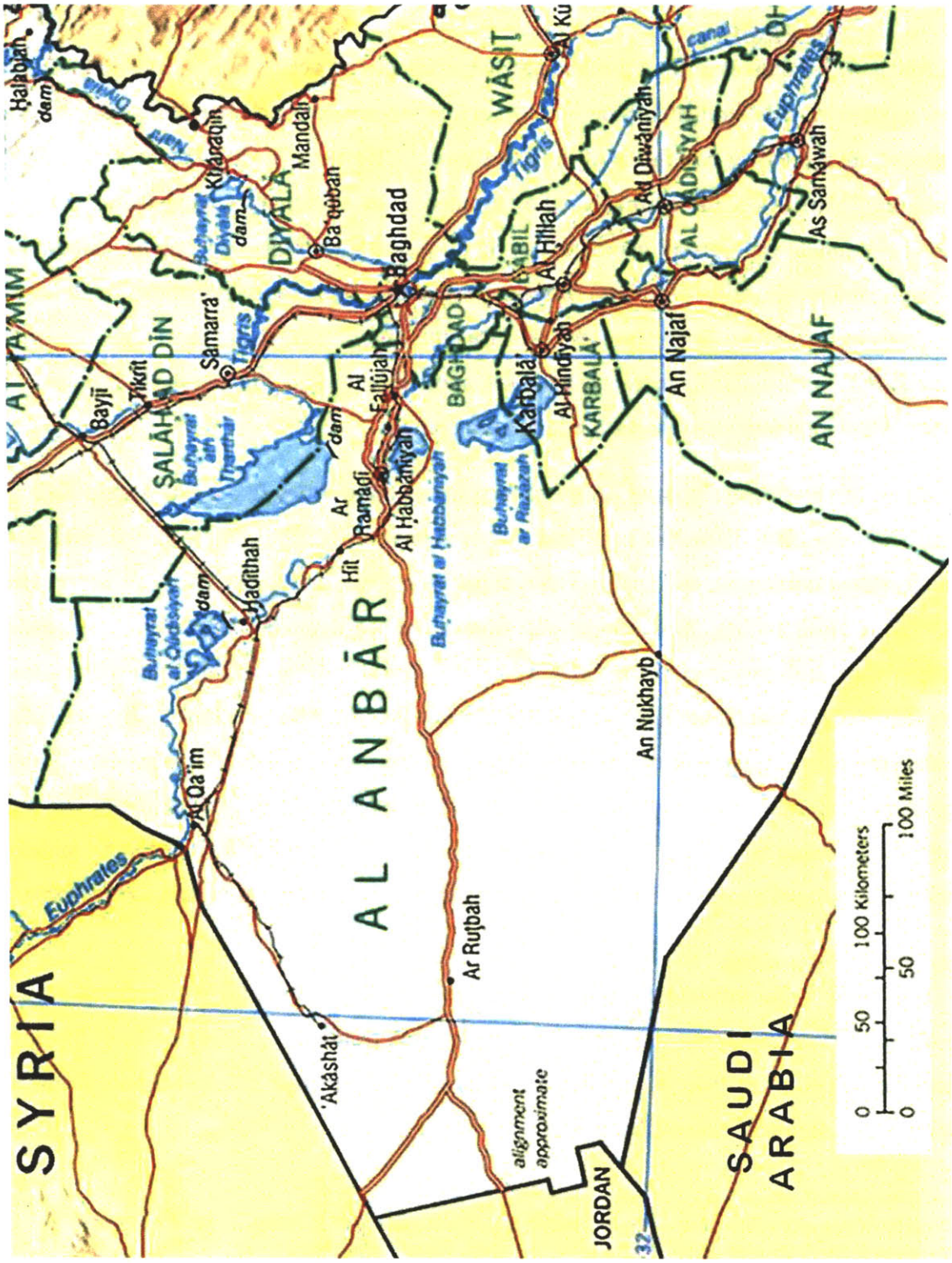


Figure 5-2: Map of Anbar Province, Iraq[16]

[16] Derived from CIA Iraq Shaded Relief Map (2004), University of Texas Perry-Castañeda Map Collection.

5.2.1.1 Sunni Anbar Explodes

Anbar was the heart of the rebellion against international occupation. The American-led invasion toppled the predominantly Sunni Baath regime and empowered previously marginalized Shia, who represented over two thirds of the population.[17] Nationalist resistance included Sunni tribesmen and former regime elements who resented both coalition occupiers and the new Baghdad government of "Persian usurpers," as Sunni referred to Iraqi Shia. Sunni nationalists were soon joined by an influx of foreign (non-Iraqi) jihadists, some loosely affiliated with the al-Qaeda terrorist network, who brought a virulent Sunni extremist tenor to the war. Fundamentalism and nationalism reinforced one another, especially in Fallujah, "the city of mosques," which had a large conservative Sunni population.

Some of the fiercest fighting in all of Iraq occurred in cities like Fallujah and Ramadi between 2004 and 2006. The war took its most ominous turn in early 2006 as it shifted from resistance against occupation to a brutal civil war between Sunni and Shia. The notorious "emir" of al-Qaeda in Iraq (AQI), Abu Musab al-Zarqawi, fanned sectarian fires with video-taped beheadings and the destruction of the Golden Mosque, one of the major Shia holy sites in Iraq. AQI staged attacks from Anbar against Shia targets in the greater Baghdad area. By the end of 2006, Marine Corps assessments of prospects for the province were outright pessimistic. Despite scoring some important successes like the killing of Zarqawi by SOF in June 2006, the U.S. appeared to be losing in Anbar.[18] The pessimistic domestic debate around the U.S. midterm elections that year sent a message to Sunni nationalists that the occupier was ready to go home.

5.2.1.2 Tribal Awakening

In a remarkable turnaround only a year later, pundits and officials touted Anbar as a model of counterinsurgency success. Violence plummeted from a high of nearly 2000 incidents in September 2006, more than in any other province in Iraq, to just 155 in January 2008, the lowest rate since the beginning of the insurgency (Figure 5-3).[19]

---

[17] On status inversion as a cause of resentment leading to civil war see Roger D. Petersen, *Resistance and Rebellion: Lessons From Eastern Europe* (Cambridge University Press, 2001), 33-36

[18] Thomas Ricks, "Situation Called Dire in West Iraq: Anbar Is Lost Politically, Marine Analyst Says," *Washington Post* (11 September 2006); Dafna Linzer and Thomas E. Ricks, "Marines' Outlook in Iraq: Anbar Picture Grows Clearer, and Bleaker," *Washington Post* (28November 2006), A1.

[19] Anbar violent Significant Activities (SIGACTs), which include direct fire attacks, indirect fire, improvised explosive device (IED) detonations and IED discoveries: US Multinational Force West (MNF-W) figures, in Anthony H. Cordesman, "Violence in Iraq: Reaching an 'Irreducible Minimum'," Center for Strategic and International Studies

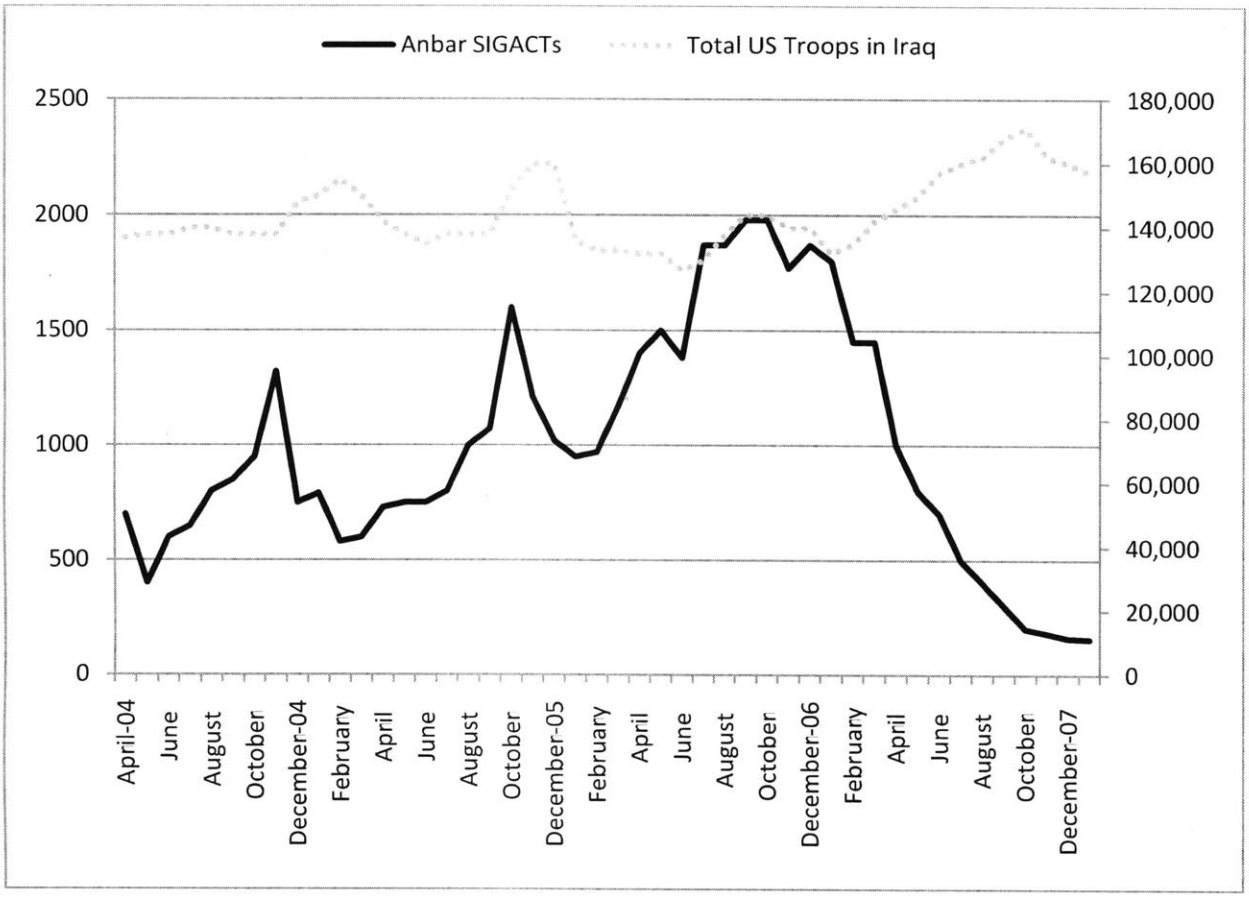


Figure 5-3: Monthly SIGACTS in Anbar (left) and overall US troop levels in Iraq (right), 2004-2007

By the time the vaunted "surge" of additional American troops began in mid-2007, Anbar province was already well over the tipping point toward stability, and similar "Awakenings" were gathering momentum outside of Anbar. While the surge augmented this momentum and helped secure Baghdad with an emphasis on population security, it did not bring about the grand bargain among Iraqi factions that its architects envisioned. The pacification of Anbar, like the

---

(25 February 2008), http://www.csis.org/media/csis/pubs/080227_violence.in.iraq.pdf. Troop strength: Michael E. O'Hanlon and Jason H. Campbell, "Iraq Index: Tracking Variables of Reconstruction & Security in Post-SaddamIraq," Brookings Institution (28 May 2009), http://www.brookings.edu/iraqindex. At the highpoint of violence in Anbar in October 2006 (corresponding to the Battle of Ramadi), about 1,980 SIGACTS, there were 144,000 US troops in Iraq. The first month in which troop totals exceeded this was April 2007, a minor increase to 146,000, and yet Anbar SIGACTS had already fallen by half to 1,000. By July SIGACTs were halved yet again, while US troops increased only to 160,000. Monthly troop totals for Anbar alone are not publically available at the time of this writing, but they would show far less of an increase (from a rough average of 35,000), given that over half of the additional "surge" troops were deployed in Baghdad. It is also notable that the surge is a gradual, steady increase from 132,000 troops in January 2007 to a height of 171,000 in October, rather than the sharp step function assumed by popular accounts. Anbar SIGACTs by contrast drop precipitously in the same period. Note that the two previous upticks and reductions of Anbar violence (corresponding to the 2004 Battle of Fallujah and the 2005 Battle of al Qaim respectively) also *precede* the introduction of additional U.S. troops, further evidence against any simple causal relationship between troop levels and violence levels.

general improvement in Iraq as a whole, grew out of bottom-up negotiations with roots that predated U.S. troop increases.[20]

The causes of the dramatic turnaround in Anbar and the degree of American agency in bringing it about remain open historical questions, but the outlines can be sketched.[21] Starting on the Syrian border in late 2005 and intensifying in Ramadi through 2006, U.S. forces began working with Sunni tribesmen—many of whom had previously fought against Americans—to combat a common AQI enemy. The skirmishes between tribal militias and AQI elements, a mixture of foreign fighters and Iraqi radicals, first erupted over control of lucrative smuggling networks along the Euphrates River corridor, which the tribes traditionally controlled. The tribes proved no match for AQI on their own, however, and tribal fighters and elites suffered badly. After unsuccessfully trying to take on AQI on their own, Albu Mahal tribesmen eventually turned to U.S. Marines for assistance, leading to the first solid setbacks for AQI in battles in and around the border town of al-Qaim.

By 2006 similar tribal alliances with American forces were emerging in Ramadi, to include the more well-known Anbar Awakening (*Sahawa al-Anbar*) movement. Alliances formed haphazardly through low-level negotiations on the initiative of local tribal elite and junior- and mid-grade U.S. officers. U.S. combat power and Anbari tribal organizations alone had been vulnerable to AQI's ferocity because Americans could not find AQI and the tribes could not stand their ground against AQI. The tribes were able to provide local intelligence and

---

[20] I make this argument further in Jon Lindsay, "Does the 'Surge' Explain Iraq's Improved Security?" Massachusetts Institute of Technology Center for International Studies, Audit of the Conventional Wisdom, September 2008. On the politics of the surge see Bob Woodward, *The War Within: A Secret White House History 2006-2008* (New York, NY: Simon & Schuster, 2008). For an analysis of the Wikileaks-disclosed data on violence in Iraq, highlighting the role of ethnic cleansing preceding the Awakening and surge, see Sabrina Tavernise, "Mix of Trust and Despair Helped Turn Tide in Iraq," *New York Times* (23 October 2010)

[21] The best accounts to date of the Awakening are: Austin Long, "The Anbar Awakening," *Survival* vol. 50, no. 2 (2008): 67-94; John A. McCary, "The Anbar Awakening: An Alliance of Incentives," *The Washington Quarterly* vol. 32, no. 1 (2009): 43-59. Other accounts tend to attribute too much agency to American efforts (vice political calculations and initiative of Anbari elites) but nonetheless provide useful detail: Niel Smith and Sean Macfarland, "Anbar Awakens: The Tipping Point," *Military Review* (Mar 2008); Bing West, *The Strongest Tribe: War, Politics, and the Endgame in Iraq* (New York: Random House, 2008); Dick Couch, *The Sheriff of Ramadi: Navy SEALs and the Winning of Anbar* (Annapolis, MD: Naval Institute Press, 2008); Thomas E. Ricks, *The Gamble: General David Petraeus and the American Military Adventure in Iraq, 2006-2008* (New York: Penguin Press, 2009); Thomas R. Searle, "Tribal Engagement in Anbar Province: The Critical Role of Special Operations Forces," *Joint Forces Quarterly*, no. 50 (2008): 62-66; Mark F. Cancian, "What Turned the Tide in Anbar?" *Military Review* (September-October 2009)

mobilize manpower for municipal police and self-defense forces, which Coalition Forces leveraged to decimate AQI throughout its strongholds along the Euphrates.

Violence spiked in 2006 as AQI waged a vicious campaign of intimidation and beheadings against tribal collaborators. The climax of the war in Anbar was the battle to secure Ramadi in late 2006, which was notable for tribal vigilantism, local self-defense groups, significant physical controls on movement (such as sand berms around cities, concrete barriers partitioning neighborhoods, checkpoints, and mandatory identification cards), and U.S. combat outposts situated right in the middle of urban neighborhoods. American personnel—both SOF and conventional forces—engaged and reassured local Anbari civic and tribal leaders, helping to organize neighborhood defense organizations and rewarding collaborators with lucrative construction contracts. Popular sympathy shifted sharply against AQI even in the face of fierce retribution. In early 2007, AQI remnants were forced to shift northward to Mosul, and violence in Anbar dropped precipitously.

Events in Anbar inspired irregular militias outside of Anbar (loosely referred to as "Sons of Iraq" with both Sunni and Shia variants) to take the fight to insurgents in other parts of the country, contributing to a similar diminution in violence nationwide. As violence subsided in 2007, U.S. forces renewed their emphasis on building government capacity, worked to demobilize militias and integrate them into police and security forces, and encouraged tribal elite to participate in legitimate politics. Within Anbar, insurgency gave way to political competition, and the province transitioned peacefully to Iraqi control in August 2008. While this did not resolve the deep rift between the Sunni province and the Shia-dominated central government, the emergence of stability and its endurance was nonetheless remarkable.

5.2.1.3 Ironies of the Awakening

A conventional wisdom has emerged that AQI brutality was the reason for the tribal "awakening" and shift of allegiance. However, AQI violence was actually a retributive consequence—not a cause—of the shift of tribal alliances. Tribal elites made rational calculations about smuggling income and their political future under a Shia government. For former Sunni insurgents, the choice to cooperate with Americans was the least of three evils, compared with AQI rule or acquiescence to the central government in Baghdad. American

overtures did not cause their decisions. Similar U.S. offers had been largely ignored in the early years of the war because it was not in the interests of tribal elite to negotiate at that time.

One irony of Anbar is that the U.S. had to lose in order to win. Put crudely, the nationalist AQI-tribal alliance politically defeated the U.S. by late 2005 or early 2006. That partnership split up on the eve of victory over a feud for control of lucrative smuggling. The tribes then recruited the considerable combat power of the political loser to vanquish its new AQI rival. In the impeccable Bedouin logic, "the enemy of my enemy is my friend." A counterargument to this story is that tenacious U.S. Marines proved to Sunni nationalists that they couldn't win militarily while also allowing them to make an honorable stand against the occupier. Indeed, something like this probably helped facilitate the realignment of alliances once interests had shifted, but it doubtfully caused the shift in the first place. The tribes had work for U.S. forces to do before they left Anbar, once it was clear that they were in fact going to leave.

A second irony is that the U.S. reinforced traditional patronage networks rather than focusing exclusively on Iraqi state capacity. American counterinsurgency doctrine, distilled in the manual authored under the leadership of General David Petraeus, cautions against bolstering militias because it undermines the legitimacy of the government.[22] However, American forces empowered and awarded no-bid contracts to tribal elites who controlled their own militias and who were hostile to the central Shia state. Bolstering the local patronage systems turned out to be a critical precondition for the success of the Petraeus surge. Put crudely again, Americans embraced a form of corruption. While non-state militias do indeed pose a long-term threat to state legitimacy, civil war is a contest of local power-consolidation (rather than an airing of broad grievances) where the state is just one actor among many.[23]

The U.S. lost before it won, and it bribed tribal militias in order to do so, all before the surge could make a bit of difference. These ironies call into question the degree of U.S. agency in winning Anbar as well as the popular surge-based narrative of American victory in Iraq. Both

---

[22] *Field Manual No. 3-24: Counterinsurgency* (Washington DC: Department of the Army, 2006) not only does not recommend leveraging tribes, community organizations, or other traditional networks to actively counter insurgent violence, it specifically characterizes irregular units as obstacles to ending an insurgency (*e.g.*, para 3-112 states, "If militias are outside the [host nation] government's control, they can often be obstacles to ending an insurgency.").

[23] Stathis N. Kalyvas, "Review: The New U.S. Army/Marine Corps Counterinsurgency Field Manual," *Perspectives on Politics* vol. 6, no. 2 (2008): 351-353; *idem, The Logic of Violence in Civil War* (Cambridge University Press, 2006)

the Bush and Obama administrations simply transposed the surge model to Afghanistan, where it seems not to be faring as well and where another Awakening miracle seems unlikely.[24] The fact that we still have a hard time explaining why things took a turn for the better in Iraq should underline the fundamental inscrutability of the SOTF's external environment in Anbar.

The ultimate legacy of the dearly-bought American adventure in Iraq remains questionable. The country could either relapse into civil war or turn into a Shia version of Saddam Hussein's autocracy, to say nothing of the complicated Kurdish question in the north. Both outcomes are not only bad for Iraqi democracy and American balance sheets but also complicate the balancing of Iranian ambitions in the region. Nonetheless, ethnically homogenous and oil-free Anbar will probably remain relatively stable and autonomous because there is little of national importance there besides Baathist retirement communities. Hard U.S. fighting and nearly a trillion dollars bought a rather tenebrous outcome.

5.2.2 The Complexity of Irregular War

Counterinsurgency battlefields are dirty. Insurgents are low-resolution targets hidden in the population. The population, moreover, is not a homogenous mass, but a complex society of local actors vying for influence and attention (or trying to avoid either). The "counterinsurgent" or the "government" are hardly above the fray, as sometimes portrayed in the counterinsurgency literature; they get actively mixed up in contests of local, almost feudal, power consolidation.[25] The presence of wealthy and capable U.S. forces amidst the poverty of wartorn Anbar introduces tremendous interaction complexity. "Corruption" of Iraqi officials becomes inevitable with the river of cash that American forces bring in for logistic sustenance and civic development. American forces that are supposed to "protect the population" create moral hazard for Iraqis interested in using American muscle to solve private grudges that have little to do with combating the insurgency.[26] Allegiances change surprisingly with powershifts at the neighborhood level. Civilians vary in their level of support for or against the insurgency, from vague ideological sympathy, to local provision of intelligence and material support, to direct

---

[24] Bob Woodward, *Obama's Wars* (New York, NY: Simon & Schuster, 2010)
[25] Colin F. Jackson, "Fighting for Feudalism? Dilemmas of State Consolidation in Iraq and Afghanistan," Paper presented at International Studies Association Annual Convention, New York, February 2009
[26] Kalyvas, *Logic of Violence in Civil War*

participation in violence.[27] Guerrillas can demobilize altogether, enter amnesty programs, or defect to the side of the government, individually or as entire factions. The extent of identity fluidity is an active area of debate in civil war scholarship,[28] and a vexing problem for counterinsurgent practitioners. Every Iraqi policeman and soldier, every municipal official, and every local contractor is a potential insurgent. Every insurgent is a potential ally or source of intelligence.

Because social networks at the level of individuals and small groups matter tremendously, the counterinsurgent must contend with far more entities, types, properties, and relationships than usually appear in conventional combat between uniformed and regimented formations. At the very least, irregular types and relationships are more dynamic and liable to emerge unexpectedly as local actors discover new ways to co-opt institutions and equipment into the fight. The counterinsurgent must pay attention to not only military ontology, but also the structure and processes of economic, legal, infrastructural and social systems in complex urban and rural settings, all of which are rife with information asymmetries and ontological instabilities. These objective problems will tend to raise information friction for counterinsurgent organizations which try to solve them.

Nevertheless, Americans enjoyed some external stability in Anbar. The Euphrates has been the dominant feature in the region for thousands of years, and only the urban areas along it really matter for state-building. The desert is so vast and inhospitable that it defeats any hope of concentration and coordination for insurgents seeking refuge there. Telephone systems, highway layouts, and the locations of dwellings are not so dynamically variable. Such structure supports more reliable representation than chaotic social networks.

5.2.3 Low-Tech Obstacles to High-Tech Possibilities

The counterinsurgency battlefield puts a premium on human intelligence (HUMINT). In order to find valuable insurgent targets, somewhere along the HUMINT cascade of inscription somebody has to have a face-to-face meeting with insurgent leaders, in order to learn who they are and to develop understandings of their patterns of life. HUMINT is a risky business rife with

---

[27] Petersen, *Resistance and Rebellion*

[28] For a thorough literature review see Paul Staniland, "Explaining Cohesion, Fragmentation, and Control in Insurgent Groups," Ph.D. dissertation, Massachusetts Institute of Technology (2010), Ch. 1.

potential for misidentification, duplicity, and exploitation for private gain. The logistics of collection against targets that don't want to be identified and tracked can be quite complicated, which lowers the chances of reliable connection. HUMINT connection is up close and personal, which makes it dangerous and hard to pull off, all more so for more important targets.

By contrast, technical collection occurs at arms-length. U.S. forces have sophisticated imagery and signals collection capabilities. Thus dwellings can be placed under surveillance, vehicles followed, and communications monitored from afar. Plenty of dead space remains for insurgents to operate in, but the existence of technical collection forces them to work harder to make sure they maintain cover and concealment in the social terrain.

Likewise, stable communication systems on a mature battlefield make it technically feasible to transport records of either technical or human collection to U.S. personnel throughout Anbar or back to the continental U.S. once records are in the system. It's important to bear in mind that technical considerations of connection and movement do not automatically lower information friction, but they do set bounds on what is possible in principle. There are many ways for creative enemies and dysfunctional organizations to undermine any type of collection.

5.2.4 The Low-Contrast Enemy

There is a basic structural asymmetry between combatants. The counterinsurgent has the positive task of stabilizing the host society and propping up the local government, while the insurgent has the negative task of simply surviving and inflicting casualties. On top of this the Americans play an offensive occupational role while insurgents play nationalist defense (somewhat more complicated in the case of foreign fighters). Robert Taber says that the guerilla fights "the war of the flea."[29] As is often said, "the insurgent wins by not losing" against its militarily stronger adversary. This asymmetry gives insurgents strong incentives to develop countermeasures to American intelligence and operations. Richard Dawkins explains the basic logic in an ecological setting: "Prey animals may end up spending relatively more of their budget on defensive weaponry than predators do on offensive weaponry. One reason for this is summarized in the Aesopian moral: The rabbit runs faster than the fox, because the rabbit is

[29] Robert Taber, *War of the Flea* (Washington, DC: Potomac Books, 2002)

running for his life, while the fox is only running for his dinner."[30] The dinner-life imbalance goes a long way toward explaining why insurgencies persist so long in the face of more militarily capable counterinsurgents: the American military in Iraq is virtually assured of its institutional survival while insurgency faces eradication. Counterinsurgent attention selects for robust, survivable, clandestine organization.[31]

The insurgency is thus strongly incentivized to complicate battlefield ontology along the lines just discussed as it seeks cover and concealment in the population and works to undermine the institutions which the counterinsurgent hopes to stabilize. The enemy is stealthy and deceptive, often infiltrating friendly forces by joining Iraqi security forces or co-opting interpreters and contractors with access to American bases. Improvised explosive device (IED) technologies and ambush tactics constantly evolve. Insurgent propaganda of their own atrocities intimidates potential Iraqi collaborators while their propaganda of American atrocities fuels local resentment and desires for vengeance. American forces relentlessly hunt insurgent leaders with regular success, but clandestine organizations prove able to regenerate new ones. Moreover, they sell their lives dearly by structuring ambushes and suicide attacks to take out as many civilians and military personnel as possible, which saps the morale of the latter.

Desperate to limit casualties, American forces emphasize strict force-protection measures such as heavily armored vehicles and large convoys for even the most routine travel. Force protection has the unintended consequence of hindering regular and informal interaction amongst the population whose hearts and minds Americans hope to win. Importantly, the enemy has to deal with similar self-inflicted wounds. All the effort to survive the counterintelligence dragnet seriously complicates insurgent coordination and communication. Moreover, insurgencies often have to recruit from the bottom of the barrel, especially as key leaders get killed off, so they end

---

[30] Richard Dawkins, *The Blind Watchmaker: Why the Evidence of Evolution Reveals a Universe without Design* (New York, NY: W. W. Norton & Co, 1996), 191-192. The rest of the passage could be taken to imply that counterinsurgent personnel worry about their fitness reports and careers after the war more than the existentially-challenged guerrilla: "Individual foxes that shift resources into other projects can do better than individual foxes that spend virtually all their resources on hunting technology. In the rabbit population, on the other hand, the balance of economic advantage is shifted towards those individual rabbits that are big spenders on equipment for running fast. The upshot of these economically balanced budgets *within* species is that arms races *between* species tend to come to a mutually stable end, with one side ahead."

[31] Derek Jones, *Understanding the Form, Function, and Logic of Clandestine Cellular Networks: The First Step in Effective Counternetwork Operations* (Fort Leavenworth, KS: U.S. Army Command and General Staff College, School of Advanced Military Studies, 2009)

up with stupid or criminal elements in their ranks that sap organizational reliability. "Battlefield promotion" is not necessarily a meritocracy. After the Awakening gathered momentum, insurgent organizations regularly fissured and had trouble trusting their records and one another. Thus while insurgent action tends to cause high information friction for the counterinsurgent, the latter also causes considerable friction for the former.

5.2.5 Hypotheses on External Stability

Table 4-3 summarizes this discussion in terms of the hypotheses about external stability from the last chapter. The net effect of the situation in Anbar is to raise information friction.

Table 5-1: Hypotheses on external stability in Anbar and SOTF information friction (XS→IF)

External Stability	Value for Anbar, Iraq	Effect on information friction
XS13. Battlefield Order	Dirty, Cluttered, Changeable	↑
XS14. Ontology	Complex, ambiguous social networks; Decent public infrastructure	↑↓
XS15. Combatant affiliation	Fickle tribal & partner allegiance, insurgents hidden in population	↑
XS16. Number	Many individuals and small groups, many types of occupations & relations	↑
XS17. Domain of combat	Cluttered urban territory	↑
XS18. Connection to entities	HUMINT complicates identification & insight; robust IMINT/SIGINT	↑↓
XS19. Movement of records	Robust U.S. communications infrastructure	↓
XS20. Enemy behavior	Deceptive, creative, regenerative	↑
XS21. Enemy attacks on information system	Subversion, infiltration, competitive propaganda	↑
XS22. Exposure of system	Robust force protection controls on movement, with overhead for interaction	↑↓
XS23. Offense/defense	U.S. on offense/occupation	↑
XS24. Information friction in enemy system	Insurgents have severe coordination and communication challenges	↓
Net Effect	**External Instability**	**High Information Friction**

5.3 Internal Consensus and Contention

The second condition for reliable information systems is that actors with a stake in the information problem must invest bureaucratic and technical resources into an integrated enterprise solution, which means they have to agree on doctrine and protocols for how they want to understand the world. By contrast, doctrinal disagreement, fragmented technical protocols,

and distorted investment increase information friction. High information friction comes in two flavors: *interference* is caused by uncoordinated actors who inflict negative externalities on one another; *insulation* is caused by excessive internal consensus that is inappropriate for an unstable environment. The SOTF suffered from both types. The complexity of the interservice and interagency U.S. counterinsurgency effort in Anbar as well as the internal fragmentation and far-flung deployment of the SOTF itself set conditions for interference. Yet the SOTF also enjoyed a degree of autonomy from conventional forces in a separate special operations chain of command, which enabled it to indulge the strong preferences for commando "direct action" inherent to U.S. SOF culture. This consensus might promote *enterprise integration* in the appropriate environment. However, the overall counterinsurgency emphasis in Anbar province, especially in 2007-2008, was on "indirect action" missions such as tribal engagement to stabilize local alliances, psychological operations to bolster government legitimacy, civil affairs to rebuild the province, and Iraqi security force training to divest their dependence on U.S. presence, rather than hunting down insurgents. Taken together, the SOTF suffered from a lot of interference in its information system, but also enjoyed an insulated consensus about what it wanted to use them for. This section will sketch out the doctrinal preferences of U.S. SOF and then the external and internal organizational complexity in Anbar.

5.3.1 The Doctrinal Preferences of Special Operations Forces

SOF is a unique subculture which has been enjoying a renaissance in the U.S. military.[32] SOF communities have austere selection programs, high levels of training, an egalitarian and meritocratic culture, greater autonomy to improvise in risky or unconventional missions, and a unique bureaucratic situation under U.S. Special Operations Command (SOCOM), "the fifth service." SOCOM, created in the 1986 Goldwater-Nichols reorganization, is unique among U.S. unified commands in having training and procurement roles like the services ("the SOF

[32] The U.S. Department of Defense defines special operations as: "Operations conducted in hostile, denied, or politically sensitive environments to achieve military, diplomatic, informational, and/or economic objectives employing military capabilities for which there is no broad conventional force requirement. These operations often require covert, clandestine, or low visibility capabilities. Special operations are applicable across the range of military operations. They can be conducted independently or in conjunction with operations of conventional forces or other government agencies and may include operations through, with, or by indigenous or surrogate forces. Special operations differ from conventional operations in degree of physical and political risk, operational techniques, mode of employment, independence from friendly support, and dependence on detailed operational intelligence and indigenous assets." Department of Defense Dictionary of Military Terms, http://www.dtic.mil/doctrine/jel/doddict (accessed 29 March 2009)

checkbook") as well as authority to conduct military operations like theater commanders. Following the Cold War and especially after 9/11, the demand for SOF has continued to increase as the U.S. put more emphasis on counterterrorism and counterinsurgency operations. SOCOM became the lead in the "global war on terror" with authority to hunt clandestine terror networks worldwide. Strong doctrinal preferences have emerged through this evolution.[33]

5.3.1.1 Direct and Indirect Action

SOCOM missions can be divided roughly into two categories: *direct action* commando exploits and *indirect action* "by, with, and through" local populations (Table 5-2). As an institution, SOCOM tends to focus on the former: high risk raids and ambushes, special reconnaissance to gather information about a target through observation or technical means, counter-terrorism to disrupt and destroy terrorist networks, and counter-proliferation to abate weapons of mass destruction threats. The latter category features, by contrast, intensive interaction with local peoples, to include training and advising irregular or guerrilla forces in unconventional warfare, foreign internal defense assistance to regular government security forces, psychological operations to persuade target audiences and shape public narratives, and civil affairs operations to conduct battlefield diplomacy and civic development initiatives.[34] The distinction between the two mission sets is often expressed in terms of "kinetic" versus "non-kinetic" operations, which accords with a general rhetorical tendency in the U.S. military to describe soft-power approaches in negative terms, *i.e.*, as *un*conventional, *ir*regular, *in*direct, *non*-lethal, or *non*-kinetic.[35] The SOF distinction is sometimes expressed more pejoratively in terms of "shooters" versus "social workers" or "snake eaters" versus "lettuce eaters."[36]

---

[33] On U.S. SOF history see David Tucker and Christopher J. Lamb, *United States Special Operations Forces* (New York, NY: Columbia University Press, 2007); *United States Special Operations CommandHistory* (MacDill AFB, FL: USSOCOM History and Research Office, 2007); Susan L. Marquis, *Unconventional Warfare: Rebuilding U.S. Special Operations Forces* (Washington DC: Brookings Institution Press, 1997); Austin G. Long and Colin F. Jackson, "The Fifth Service: The Rise of Special Operations Command," in *US Military Innovation After the Cold War: Creation Without Destruction*, ed. Harvey M. Sapolsky, Benjamin H. Friedman and Brendan Rittenhouse Green (Routledge, 2009)

[34] See my appendix on U.S. SOF

[35] The positive term "hybrid operations" is gaining some currency in contemporary military discourse.

[36] These are, of course, false dichotomies: a special reconnaissance mission on its own is, strictly-speaking, non-lethal even though it may provide information for a kinetic target; an unconventional warfare effort may involve lethal action by indigenous paramilitaries; a civil affairs project might provide cover for intelligence collection which leads to a direct action raid, which is conducted for psychological effect. Both mission sets require strong teamwork, discretion, problem solving, and tactical proficiency. The indirect missions furthermore require cultural and political savvy, which can in principle also support direct action missions.

Table 5-2: SOF Direct and Indirect Action Missions and Forces

	Direct Action	Indirect Action
Missions	Direct Action (Raids, Ambushes) Special Reconnaissance Counter-Terrorism Counter-Proliferation	Unconventional Warfare Foreign Internal Defense Psychological Operations Civil Affairs Operations
Forces	Special Mission Units Naval Special Warfare (SEALs)[37] Rangers Special Operations Aviation	Special Forces (SF) Psychological Operations Group Civil Affairs Brigade Special Operations Aviation

5.3.1.2 An Overemphasis on Direct Action

While the missions overlap, the polarization between them is nevertheless strong, with discernable revealed preferences for direct action. While SOCOM was created to be an advocate for all unconventional capabilities, the meteoric rise of SOCOM following the Cold War has not benefitted all of its parts fairly.[38] There are three reasons for this pronounced bias.

First, military organizations generally prefer offensive doctrines because they reduce uncertainty and enhance bureaucratic resources and autonomy.[39] Direct action missions provide immediate and clear feedback of mission success or failure. Given the complexity and risk of sending small numbers of men into dangerous and potentially out-numbered situations, mistakes are costly in terms of lives and national embarrassment, as SOF debacles in Iran in 1980 or Somalia in 1993 illustrate. SOF thus train hard for the most dangerous and risky missions in order to get them right. Such missions also involve a repertoire of standardized tactics, techniques, and procedures, which makes reliable training and evaluation possible; this is especially helpful when faced with the large influx of new recruits SOF has had to incorporate in the decade after 9/11. By contrast, advisory, civil affairs, and persuasion missions are messy,

---

[37] Naval Special Warfare (NSW) consists mainly of SEAL (SEa, Air, and Land) frogmen, but also Special Warfare Combat Crewmen (SWCC) to helm small fast boats as well as a large cadre of support personnel.

[38] For an overview of the missions and forces in Table 18 and of the direct action bias or "graying" of SOCOM (a reference to the drift of overt "white" SOF, which tend to conduct indirect action or unconventional warfare, toward classified "black" special mission units specializing in direct action), see Austin G. Long and Colin F. Jackson, "The Fifth Service: The Rise of Special Operations Command," in*US Military Innovation After the Cold War: Creation Without Destruction*, ed. Harvey M. Sapolsky, Benjamin H. Friedman and Brendan Rittenhouse Green (New York, NY: Routledge, 2009); Tucker and Lamb, *USSOF*

[39] Barry R. Posen, *Sources of Military Doctrine: France, Britain and Germany Between the World Wars* (Ithaca, NY: Cornell University Press, 1984), 47-50; Jack L. Snyder, *The Ideology of the Offensive: Military Decision Making and the Disasters of 1914* (Ithaca, NY: Cornell University Press, 1989)

drawn-out projects that require extensive inter-organizational and cross-cultural collaboration. They require maturity, judgment, empathy, and cultural and linguistic fluency, all of which are expensive life skills not easily trained in a schoolhouse curriculum. While less physically risky, indirect missions by the same token feature much more ambiguous feedback. In sum, direct action missions promise to reduce uncertainty and enhance autonomy, while indirect missions are ambiguous and involve lots of inter-organizational interference.

Second, SOF outfits and Naval Special Warfare especially cultivate a warrior identity. The community is permeated with valorous images, trophies, and lore to reinforce the brotherhood's identity, further bolstered by countless Hollywood action flicks, first-person-shooter video games, and published tales of derring-do.[40] Intensely competitive selection processes, such as such as Basic Underwater Demolition/SEAL training (BUD/S) emphasize physical endurance, teamwork, and mission-accomplishment at all costs. Over three quarters of those who start BUD/S drop out, either because they get injured in the grueling training or because they "ring the bell," a humiliating ritual of defeat for "BUD/S duds." Graduates earn the right to wear a large golden "trident" insignia.[41] A life-changing shared experience, BUD/S forges a powerful in-group dynamic, and the SEAL community continually reinforces its message: you are better than other men because you never quit.[42] While the cult of the frogman actively construes direct action as a path to glory, indirect missions, by contrast, have lower prestige, less arduous selection programs, and are usually performed only grudgingly by operators.[43] Support personnel and indirect action specialists rank well below commandos on the SOF totem, as will be discussed more below in the section on expedient adaptation.

---

[40] For a typically hagiographic overview of the SEAL community see Mir Bahmanyar and Chris Osman, *SEALs: The US Navy's Elite Fighting Force* (Oxford: Osprey Publishing, 2008). SOF's fearsome reputation can be helpful in the field, of course. On one operation in Iraq, the targeted individual happened to be watching the film *Under Siege*, in which Steven Segal plays a lone SEAL on a hijacked vessel, when the real assault team came through his door. He smiled and calmly surrendered without a fight.

[41] Also called a "Budweiser," the trident is physically the largest warfare-qualification badge in the Navy and one of the few gold-colored devices worn by both officer and enlisted personnel; most other enlisted devices are silver. This symbolizes that both officers and men have gone through the same training, are capable of the same tactical leadership, and demonstrates a more egalitarian military subculture than found elsewhere in the Navy.

[42] For a detailed account of BUD/S see: Dick Couch, *The Warrior Elite: The Forging of SEAL Class 228* (New York: Three Rivers Press, 2001)

[43] Even the unique "Robin Sage" portion of SF training focusing on indigenous interaction has reportedly been deemphasized in recent years; see Austin G. Long, "First War Syndrome: Military Culture, Professionalization, and Counterinsurgency Doctrine," Ph.D. dissertation, Massachusetts Institute of Technology, 2010

Furthermore, the often overt nature of indigenous engagement is at odds with SOF's traditionally clandestine modus operandi.

Third, civilian political leadership reinforces SOCOM's internal preferences through funding and officer promotion. Clandestine and covert operations are tempting tools for elected officials looking for quick fixes to difficult foreign policy problems.[44] SOCOM's commanders and senior leadership have generally been drawn from elite special mission units and Rangers with high-risk counterterrorism missions.[45] SOCOM's counterterrorism budget and influence increased after 9/11 with enthusiastic support from the Bush administration.[46] It helps to have an excited patron with deep pockets. The Obama administration maintained this strong support by significantly increasing the SOF presence in Afghanistan under General Stanley McChrystal.[47] Even though many SOF professionals acknowledge that indirect missions are critical to the types of counterinsurgency and stabilization missions most likely to challenge the U.S. military in coming decades, there is no comparably interested patron to champion those capabilities.[48]

All of the above factors—organizational incentives, SOF identity, and civilian patronage—reinforce a SOF bias toward direct action. The preference is over-determined bureaucratically, culturally, and historically. As a general rule, military forces tend to resist embracing the population-focused indirect missions associated with counterinsurgency.[49] SOCOM tends to reinforce conventional military approaches to war, which is rather ironic given that SOCOM was created in order to protect unique SOF capabilities from marginalization by the conventional services. Hy Rothstein aptly describes direct action as "hyper-conventional," because it pursues familiar types of military objectives, just with greater speed, proficiency, risk, money, and secrecy. The indulgence of traditional military preferences is a far cry from truly

---

[44] John Prados, *Presidents' Secret Wars: CIA and Pentagon Covert Operations since World War II* (New York, NY: W. Morrow, 1986)

[45] Sean D. Naylor, "More than door-kickers," *Armed Forces Journal* (March 2006)

[46] Bob Woodward, "Why Did Violence Plummet? It Wasn't Just the Surge," *Washington Post* (8 Sept 2008): A9; Andrew Feickert, "U.S. Special Operations Forces (SOF): Background and Issues for Congress," Congressional Research Service, Library of Congress (16 May 2008)

[47] Michael Hastings, "The Runaway General," *Rolling Stone* (1108/1109 2010), http://www.rollingstone.com/politics/news/17390/119236

[48] Tucker and Lamb, *United States Special Operations Forces*; Sean D. Naylor, "Success against enemy not measured in kills, says terrorism official," *Army Times* (4 December 2006); Sean D. Naylor, "Support grows for standing up an unconventional warfare command," *Armed Forces Journal* (September 2007)

[49] Colin F. Jackson, "Defeat in Victory: Organizational Learning Dysfunction in Counterinsurgency," Ph.D. dissertation, Massachusetts Institute of Technology, 2008

unconventional or "special" approaches which work "by, with, and through" indigenous populations. This institutional distortion directs attention away from long-term unconventional efforts that might better manage the political risks and opportunities in counterinsurgency than the outsized emphasis on high-risk, short-turnaround commando raids. While SOCOM was created to protect SOF from conventional forces, it ironically promotes their convergence.[50]

5.3.1.3 Doctrinal Misalignment in Anbar

The first Naval Special Warfare (NSW) Task Unit arrived in Ramadi in 2005, followed by a larger Task Group headquarters to Fallujah in 2006, renamed a Special Operations Task Force (SOTF) later that year.[51] While the Task Units were responsible for training Iraqi security force partner units, and while a few SEALs did participate in tribal engagement initiatives, the overriding NSW focus throughout 2006 and into 2007 was on direct action operations to kill or capture insurgents.[52] Given the intensity of the battle of Ramadi and the inherent lethality of SEALs, this was a reasonable priority, but it was the "non-kinetic" cultivation and reassurance of local allies by Army and Marine battalions that turned the tribal opening to negotiation into AQI defeat. SEALs focus almost entirely on preparing for direct action missions in their eighteen months of inter-deployment training, which makes them some of the best commandos in the

---

[50] Hy S. Rothstein, *Afghanistan and the Troubled Future of Unconventional Warfare* (Annapolis, MD: Naval Institute Press, 2006). A complementary point developed in Tucker and Lamb, *United States Special Operations Forces*, is that SOF direct action forces tend to be early adopters of tactics and equipment which will percolate into conventional ground forces, which then tend to become more SOF-like over time with advances in technology and training (*e.g.*, the use of night-vision devices, unmanned vehicles, individually-customized weapons, and small-unit interaction with the locals by increasingly well-educated soldiers and Marines). Raymond T. Odierno, Michael E. Brooks and Francesco P. Mastracchio, "ISR Evolution in the Iraqi Theater," *Joint Forces Quarterly*, no. 50 (2008): 51-55, notes that conventional infantry units are increasingly able to conduct time-critical, intelligence-supported SOF-like raids. Thus, while SOF direct action has a comparative advantage through its tighter coupling of reconnaissance and strike, this remains a difference in degree rather than kind.

[51] An NSW Task Unit ("TU") is a company equivalent formation commanding multiple NSW Task Elements or Detachments ("Dets"), which are drawn from SEAL Platoons and/or Small Boats Units, mini-submarine units, intelligence activities, and other enabling capabilities. An NSW Task Group ("TG") is a battalion equivalent formation commanding multiple Task Units. A Task Group is generally composed of an NSW Squadron ("NSWRON"), which is the deployed formation of a SEAL Team (six SEAL Platoons of about eighteen operators each) plus some additional "enablers" for communications, intelligence, logistics, *etc.* drawn from the NSW Groups based in Coronado, California and Little Creek, Virginia. An NSW Squadron can thus have two or three times as many people as a SEAL Team. The NSW Squadron is a relatively recent construct implemented with the "NSW 21" reforms of 2000, prior to which individual SEAL Platoons generally deployed and attached to traditional Navy commands with limited logistic or intelligence support of their own.

[52] Couch, *Sheriff of Ramadi*, sympathetically chronicles the operations of the NSW Task Unit in Ramadi from mid-2005 through mid-2007. He relates that the SEAL focus on sniper operations made them deliberate targets of insurgent attacks; such operations were curtailed because they seemed to be generating too much unproductive fighting rather than their intended purpose of protecting soldiers.

world.[53] Thus when SEALs deploy they want to "run to the sound of the guns," itching to get into a kinetic battle. If they find themselves in a different kind of war, they are often frustrated and disappointed. As one operator explained, "SEALs are like thoroughbred horses, and when you put them on the racetrack they want to run."

During the 2007-2008 timeframe of this study, the overall American emphasis in Anbar had already shifted from fighting insurgents to capitalization on the momentum of change and consolidation of newfound stability. The tactics which helped to promote (but not cause) the Awakening in Anbar—tribal engagement, unconventional warfare with irregular proxies, security force training, civil-military operations—are all examples of indirect action. With AQI by and large pushed out of the cities and into rural redoubts, Army and Marine "battlespace owners" shifted their emphasis to the encouragement of militarized tribal groups to pursue a peaceful political process and enhancement of the capability and legitimacy of Iraqi Army and Police. Conventional units performed the important indirect action efforts while the smaller SOF units tend to focus more on direct action. SOF, especially Army "green berets," have a popular reputation for excelling at unconventional warfare. Yet in Anbar the conventional forces undertook the lion's share of training Iraqi forces and negotiating with local elites, so SOF concentrated more on raids. There remained some irreconcilable elements and AQI remnants to clean up, but the former assumed more importance *vis-a-vis* the long term stability of the province. SOF doctrinal preferences were thus at odds with the overall counterinsurgency emphasis in Anbar.

In the early years of the Iraq war, the Army and Marines went through a very painful and public learning process to deemphasize killing the enemy and to instead embrace the "hearts and

---

[53] By comparison Army Special Forces soldiers, who typically are older than SEALs when they go through their initial selection course, only have five or six months between their seven month deployments to Iraq or Afghanistan. This has the effect of maintaining a higher degree of cultural literacy for SF. The eighteen month SEAL interdeployment training cycle has three phases. During the first six months of "professional development," operators attend individual schools (i.e., sniper, jumpmaster, demolition, communications), followed by six months of "unit level training" during which each SEAL Platoon trains as a team. The goal of this first year is proficiency in executing a "full mission profile" from initial planning through all the phases of a direct action or special reconnaissance mission (*i.e.*, insertion, infiltration, actions on the objective, exfiltration, and extraction) on land or at sea. In the next six months SEAL Team (six Platoons) preparations for deployment begin in earnest with "squadron integration training" during which the Platoons learn to work together within a broader command framework involving larger-scale exercises and battle staff drills and absorbing lessons-learned from whichever Team has most recently returned from deployment.

minds" approach exemplified in *Army Field Manual 3-24*. By 2006 and certainly by 2007, the gospel according to David Petraeus had been widely embraced as the new conventional wisdom for irregular warfare throughout most American forces. Remarkably, the contrary SOF subculture has not only persisted but even further indulged its preferences for direct action during the same period. The "conventionals," in the pejorative SOF term of art, have embraced unconventional warfare while "special" operators have become hyper-conventional. This ironic curiosity attests to the robustness of the bureaucratic, ideological, and historical factors which shape American SOF institutions. The counterargument to my criticism of this doctrinal mismatch is that the division of labor is complementary. Large conventional forces that win hearts and minds provide intelligence about and limit the regeneration of the insurgents which SOF hunts. SOF direct action keeps pressure on insurgent networks to protect conventional state-building efforts. There is surely some truth to these synergies, but such arguments were made just as often to relieve SOF of having to think through the unintended consequences of their myopic fascination with direct action.[54]

5.3.2 The Crowded Counterinsurgency

The American-led intervention in Iraq was a complicated tangle of military, civilian, corporate, nongovernmental and international organizations. SOF formed only a small part of this menagerie, but they interacted with many different kinds of actors in overlapping chains of command, depicted in Figure 5-4.[55] The SOF preference for direct action was often at odds with what had become by 2007-8 a thoroughly indirect action mission led by the Marine Corps.

---

[54] For various takes on the relationship between SOF and conventional forces see Gary Luck and Mike Findlay, "Special Operations and Conventional Force Integration," United States Joint Forces Command, Joint Warfighting Center, Focus Paper no. 5 (2008); US Special Operations Command Pub 3-33, *Conventional Forces and Special Operations Forces Integration and Interoperability Handbook and Checklist* (MacDill Air Force Base, FL: 2006); Joseph D. Roller, "Leaders Wanted: SOF and CF Integration," Air Command and Staff College Paper (2006)

[55] SOTF components, depicted with bold borders, have different names depending on whether it is an Army SF or Navy SEAL unit. Solid lines depict command authority, and dashed lines are coordination relationships. Ranks of commanders of military units indicated by rank insignia.

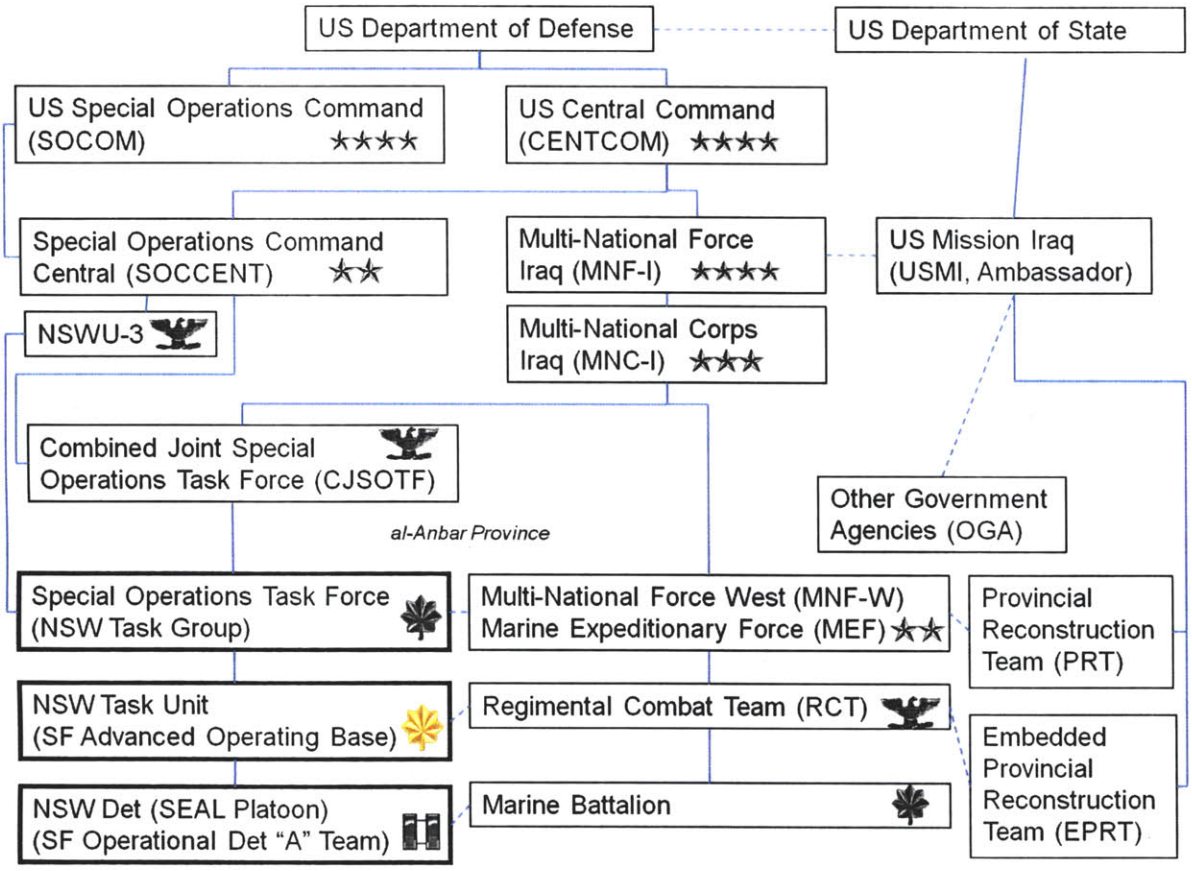


Figure 5-4: Operational command relationships of the SOTF in Anbar province

5.3.2.1 SOF Autonomy

SOF commanders enjoyed a degree of autonomy from conventional forces, some robust dedicated support assets, and a great deal of responsibility and influence for their rank.[56] They could set their own campaign objectives and react quickly to emerging intelligence opportunities.

Army Special Forces, Naval Special Warfare, and airborne lift and reconnaissance units were consolidated in a Combined Joint Special Operations Task Force (CJSOFT) north of

[56] As depicted in Figure 5-4, the SOTF was commanded by a Navy commander (O-5), operating in the same area as a two-star Marine (O-8). The Dets/ODAs were commanded by Navy lieutenants or Army captains (O-3) operating in the same area as a conventional battalion commanded by a lieutenant colonel (O-5). The CJSOTF commander was a colonel (O-6) responsible for all of Iraq, giving him a unique perspective often leveraged by the four-star commanding general (O-10).

Baghdad.[57] CJSOTF ran three regional SOTFs, each manned either by an Army SF Battalion, or in the case of Anbar, by a Navy SEAL Squadron.[58] The latter was accountable to three different masters in California, Bahrain, and Iraq, respectively, each of which imposed unique reporting requirements.[59] A SOTF could have additional attached capabilities such as civil affairs or psychological operations teams, but the Anbar SOTF did not have these at the time and so such functions were performed *ad hoc* by augmentees.

The SOTF maintained a broad mission portfolio, complementary to the larger Marine effort. Each Task Unit trained one or more partner forces, usually Iraqi Army or Police special units, and kept up liaison with local sheikhs, in coordination with broader Marine engagement initiatives. Figure 5-5 shows a slide that I put together early in the deployment to illustrate to the SOTF staff and visitors how different SOF missions (Table 5-2) addressed different segments of the population, as well as how SOF and conventional emphasis *ideally* differed. Direct action targeting focuses on active insurgents, with SOF focusing on networks leading to insurgent leadership. Indirect action training and engagement provide partner forces, intelligence, and enhance local capacity, which aids the targeting mission by making insurgents legible against and separable from the social background. Given the critical importance of local context and

---

[57] The "Combined" in CJSOTF signifies the inclusion of allied SOF, mainly British. During the 2007-2008 timeframe MNC-I was commanded by Lieutenant General Raymond Odierno, who reported in turn to General David Petraeus, commander of Multi-National Forces-Iraq (MNF-I), the overall military headquarters in Iraq. In late 2008 these two levels of command were merged, Odierno was promoted to full general to relieve Petraeus, and Petraeus in turn went on to command CENTCOM.

[58] A SOTF is ostensibly a Joint unit organized into three levels of command, but units usually had distinct Army or Navy personalities. Each SOTF commanded either SF Advanced Operating Bases (AOBs) manned by SF companies or NSW Task Units, which in turn controlled several SF Operational Detachment "A"Teams (ODAs) or NSW Detachments (augmented SEAL platoons). The NSW Dets were somewhat larger than the twelve-man ODAs, not only by virtue of the eighteen-man SEAL platoons, but also because of the Det's staff and support personnel, totaling perhaps forty people. The NSW interpretation of this was that the Dets were more capable than ODAs because all the dedicated enablers at the low echelon gave them more intelligence and combat power; on the contrary, the SF interpretation was that ODA personnel were more flexible and effective at COIN because they did more with less, with every soldier cross trained to do many jobs, and with more effective and intensive indigenous integration, rather than SEALs who had the luxury of just being commandos. CJSOTF and SOTF command organization are further described in Couch, *The Sheriff of Ramadi*, 17-19.

[59] The U.S. military distinguishes tactical, operational, and administrative control of forces. ADCON is responsible for manning, training, and equipping forces. OPCON, a function of theater combatant command, is responsible for positioning forces in theater. TACON is responsible for conducting tactical engagements. The different types of authority may or may not be delegable or reside in the same commander. The administrative commander of SOTF-W was the NSW Group back in the U.S., the operational commander was the NSW Unit in Bahrain, and the CJSOTF was the tactical commander. By contrast the CJSOTF was the administrative, operational, and tactical commander for Army SOTFs because the Army colonel commanding whatever Special Forces Group deployed to Iraq also assumed command of the CJSOTF. The Army SOTFs enjoyed greater unity of command.

individual motivation in internal war, the integration of engagement with both targeting and training (the -2 and +2 segments of the population) is especially important. [60]

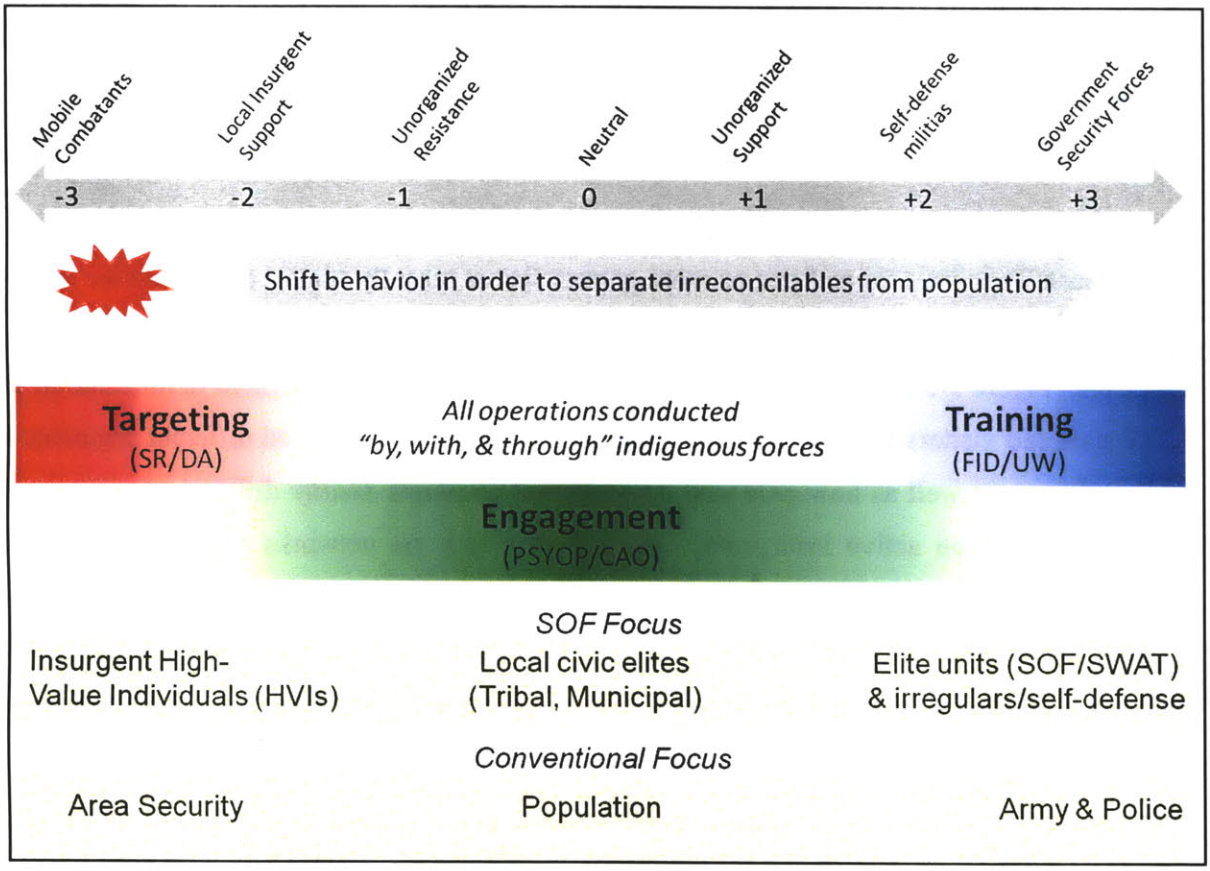


Figure 5-5: SOTF slide depicting SOF missions (listed in Table 5-2) in counterinsurgency.

In *practice*, SOTF Task Units dedicated most of their intelligence and planning resources to direct action targeting. It could be and often was argued that insurgent targeting was a comparative advantage of SOF, and so a division of labor with the Marines made sense. Furthermore, SOF needed to train partner forces to competently conduct the most dangerous and risky missions. These arguments overlooked the downsides of an exclusive targeting focus: false positives could kill the wrong people and generate antipathy; false negatives could miss dangerous insurgents because of a lack of reliable human intelligence. Indirect action had the potential to sensitize units to and help to mitigate both problems, while ignoring it also removed

[60] This slide and the concepts in it are described in more detail in my appendix on Full-Spectrum Counterinsurgency. This slide is reconstructed from memory.

a source of feedback that anything was amiss with the direct action emphasis, discussed further in Chapter 7.

5.3.2.2 Reliance on the Marine Corps

Despite its separate chain of command, SOTF ability to operate independently of the Marines was limited in practice. A Marine Expeditionary Force (MEF), a division-sized unit with its own air wing commanded by a two-star general, was the "battlespace owner" in Anbar. There were more Marines in Anbar than SOF by two orders of magnitude (over thirty thousand to about four hundred). Each of the SOTF's operating locations was a separately-secured compound within a larger Marine forward operating base (FOB). Marines provided the SOTF with combat service support functions such as base security, gasoline, chow halls, and exchanges. Conventional forces also supplied rotary wing lift for all the routine circulation among bases throughout the country (Figure 5-6).[61] The SOTF furthermore depended on Marines to provide a Quick Reaction Force (QRF) or casualty evacuation in the event a mission ran into trouble such as heavy enemy resistance or a roadside bomb. This necessitated coordination with Marines for every mission that left the base, even routine logistics runs and visits to talk with local Iraqis. The SOTF also depended heavily on Marine maps and information for all of its operations. Marines derived intelligence about people, places, and events from regular patrols throughout Anbar, Combat Outposts embedded in neighborhoods, and multiple human intelligence teams.[62] The divisional (MEF) headquarters had a robust intelligence department and "Tactical Fusion Center" employing several hundred personnel working across technical disciplines and functional areas of expertise. The Marines also had competent reach-back support from the Marine Corps Intelligence Activity (MCIA) in Quantico, Virginia.[63]

---

[61] Helicopter assault usually relied on CJSOTF aircraft from Balad, presenting planning challenges given the distances involved in Anbar and the preference of SOF air to fly only at night. Ground assault relied on the SOTF Dets' armored Humvees, and boat assault on organic SOTF watercraft.

[62] Expedient adaptation with Microsoft tools featured heavily in Marine collection and processing of patrol information; James A. Russell, "Innovation in War: Counterinsurgency Operations in Anbar and Ninewa Provinces, Iraq, 2005-2007," *Journal of Strategic Studies* vol. 33, no. 4 (2010): 595 - 624

[63] Since the Marines were deployed primarily in Anbar, the province benefitted from the attention of a service-level intelligence agency, MCIA. By contrast, the National Ground Intelligence Center (NGIC), although much larger than MCIA, had to spread its attention across Army units in all of Iraq and Afghanistan. The Marines in Anbar benefitted tremendously from having a dedicated provincial focus at MCIA.

Figure 5-6: Marine CH-53 in front of "JDAM Palace" in Ramadi (Author's photo)

Both the Marines and SEALs are part of the Department of the Navy, but they did not see the world in Anbar in the same way. The Marine Corps had a large persistent presence throughout the province, so it assumed responsibility for most of the civil-military operations. The Marines patrolled and interacted far more intensively with Iraqi locals, and they had far more resources to bring to bear for both coercive and developmental projects. As a result the Marines were far more invested with local relationships than SOF, which focused on hunting bad guys. The Marines did not formally control SOF, but SOF dependence on Marine basing, airlift, emergency response, communications, and intelligence enabled the Marines to wield influence to restrict the types of targets and areas that SOF could pursue in order to control the blowback from SOF direct action.

5.3.2.3 Organizational Complexity Promotes Insularity

The SOTF was suspended in a web of far more internal and external relationships than any organization chart like Figure 5-4 could possibly reveal. Table 5-3 lists the different organizations with which the SOTF had to coordinate, such as the State Department's Provincial Reconstruction Teams (PRTs) with the Anbari provincial government and Marine regiments,[64] other government agencies to include members of the U.S. intelligence community, and non-governmental organizations in Iraq and back in the U.S. Each of them had unique information systems, formats and requirements. There was ongoing negotiation among them with no formal authority over one another. Units might exchange liaison officers, but too often the person a unit was willing to give up would, for the same reason, not be of the best quality. Action officers might visit one another, but transit by helicopter a few dozen miles might take hours or days of coordinating through schedules and sandstorms.

Before even considering Iraqi enemies and allies—the ostensible reason for being in Iraq at all—SOTF personnel had to understand and maintain their role in the complicated internal metabolism of the US effort in Iraq. While it takes a lot of work to understand the social structure of Iraqi tribes, insurgents, and government institutions, it was nearly as hard to understand the counterinsurgent infrastructure sprawling across an archipelago of self-contained bases along the Euphrates valley. Unfortunately, the latter was perhaps more salient for most personnel trying to get through their tour and out with a favorable performance evaluation. The command complexity, ultimately responsible to no one person, generated a high volume of communications, demanded effort to manage, and ultimately turned attention inward to Coalition bureaucracy. Iraqi social structure for its part remained—in American experience but not Iraqi reality—far more undifferentiated. The complexity of Coalition Forces organization was more salient in most day-to-day military experience than the complexity of Iraqi society and the multiple fissiparous insurgencies.

Table 5-3: Actors who interacted with the SOTF

[64] PRTs worked with different echelons of military command but each reported directly to the American embassy (see Figure 24). This mismatch in command structure made for some coordination and authority challenges.

US SOF in Iraq

- Internal SOTF staff sections (admin, intel, ops, logistics, comms, medical)
- Task Units (staff sections, NSW Dets, Army ODA)
- Augmentee units: interrogators, Explosive Ordnance Disposal, Psychological Operations, Civil Affairs
- CJSOTF (HQ, staff sections, SOF air component)
- Adjacent SOTFs and ODAs
- Relieving units (turnover preparation)
- National Special Mission Units not in the CJSOTF chain of command

Other US units in Iraq

- Base life support (dining, water, fuel, sanitation, base security, medical, post, exchange, morale & recreation)
- Marine Corps Divisional (MEF) staff sections, Regiments, Battalions (airlift, ops coordination, intel, comms)
- Lateral US Army units outside Anbar
- Theater commanders (Force/Army, Corps, security force training)
- Detention facilities
- Provincial Reconstruction Teams
- Intelligence organizations

US-based entities

- Administrative force providers (situation reports, resupply, relief, awards, personnel evaluations)
- Operational Commands (NSWU-3 in Bahrain, SOCCENT in Florida)
- Reach-back support agencies (intel, ops, logistics, IT access/service)
- Distinguished Visitors/VIPs
- Visiting assessment teams (SOCOM, CENTCOM, DOD, Interagency, Congressional delegations)
- NGOs (development, humanitarian relief, servicemember support)
- Private security contractors
- Journalists (visiting, embedded, roving)

Iraqis

- Construction & supply contractors
- Interpreters
- Iraqi Army, Police, SOF partner forces
- Civic elite, municipal employees
- Tribal elite & family members
- Political parties
- Militias (tribal, sanctioned, illegal)
- Intelligence sources
- Criminals
- Insurgents (nationalist, Baathist, jihadist, sectarian)

5.3.3 Fragmentation inside the Task Force

SOTF personnel not only had to deal with coordination problems with other counterinsurgent actors but also with the tangled relationships in their own house. Altogether, the SOTF in Anbar during the study period had three Task Units (company equivalent formations), six SEAL Platoons from two different SEAL Teams, one Army Special Forces team (ODA), and a logistics detachment. Four hundred people worked across eight different operating locations. Less than a third of these were Navy SEAL or Army SF "operators," illustrating SOF's heavy reliance on support personnel or "techs." Even the operator third included many operators working in exclusively staff positions.

5.3.3.1 Last-Minute Augmentation

Most SOTF operating locations had a "battle staff" and various "enabler" functions, depicted in Figure 5-7.[65] These staffs were filled out with "individual augmentees" from SOCOM or other Navy commands and mobilized reservists, some of whom filled important positions on the staff, such as legal, air, detainee, and civil affairs. Augmentees usually lacked SOF experience, and by the same token the SEAL squadron had not really exercised their functions prior to deployment, because augmentees showed up only just before, and sometimes even just after, the squadron deployed. As supporting "techs" ranked well below "operators" on the SEAL totem, the organization invested far less in training and recruiting the former. Even intelligence functions—critical for either direct or indirect action—were a haphazard mix of organic SEAL Team personnel, augmentees, "reach back" from the continental U.S., and various novel special purpose units bolted on at the last minute.

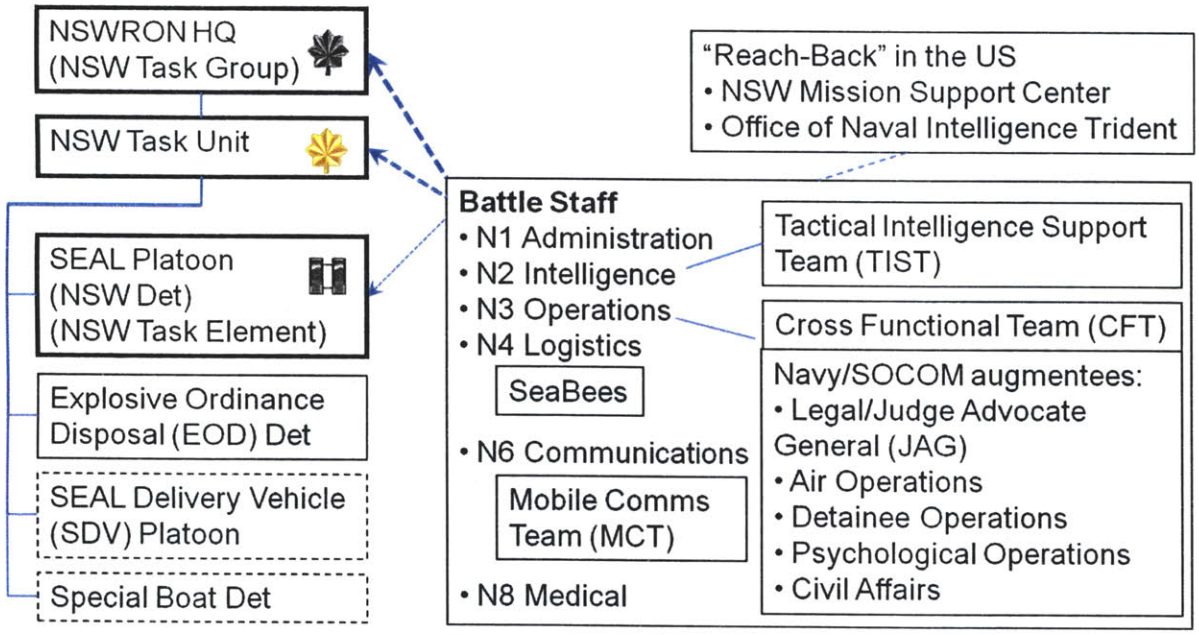


Figure 5-7: SOTF and NSW squadron (NSWRON) organization

The squadron arrived in theater with SEALs ready to conduct direct action after eighteen months of dedicated training, but its knowledge-management and indirect action capabilities

[65] Each of the command elements (in bold) has a battle staff (N-codes) with various functional enablers from other force providers added on. This is an idealized depiction as particular Naval Special Warfare Squadron (NSWRON) configurations are tailored to operational circumstances, as for example, there was little need for SEAL delivery vehicles (SDV minisubmarines) or boat units in the Anbari desert.

were a pick-up game. Furthermore, some of the SEAL Team's platoons had actually deployed to a completely different theater to meet other SOCOM requirements, which complicated preparation for the deployment and undermined the concept of the squadron as a coherent unit. Without any standard doctrine for integration, each squadron felt its way through organizing its information processes differently with whoever happened to show up. The turbulence of last-minute personnel augmentation with little quality control raised information friction considerably.

5.3.3.2 Office Space

The physical setting of the SOTF provided informational boundaries and resources above and beyond the contents of digital servers.

Figure 5-8: NSW Task Unit collocated with SOTF (Author's photo)

As visitors and SOTF personnel came and went, they interacted with people, paper charts on the wall, and computer systems that could only be accessed locally. The SOTF occupied a

separate walled compound within a larger Marine forward operating base (FOB). It was a temporary, expeditionary facility (Figure 5-8 is typical), although its infrastructure grew more robust as time passed.

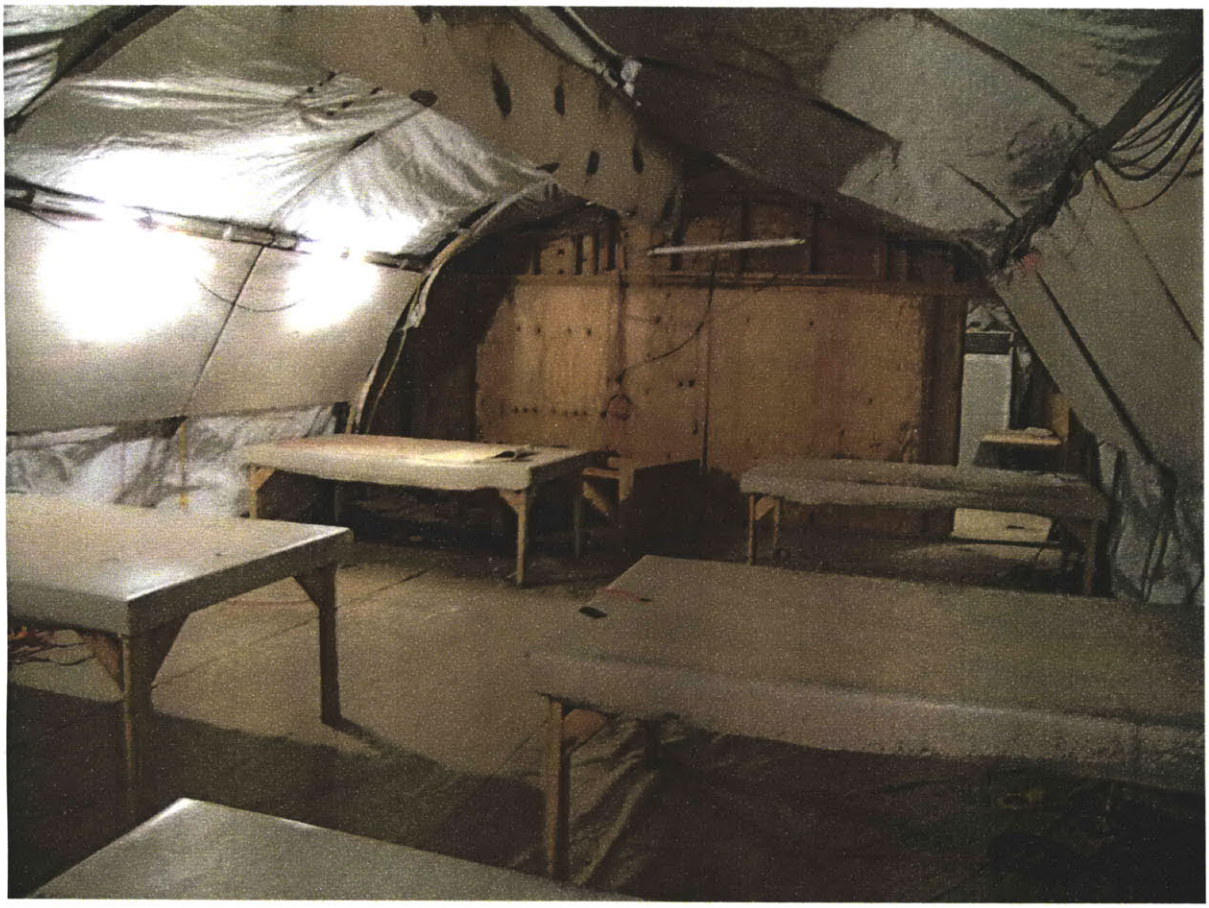


Figure 5-9: Interior of an Alaskan Shelter tent at the SOTF HQ, sans equipment (Author's photo)

The camp had air-conditioned Alaskan Shelter tents (Figure 5-9), modest wooden buildings constructed by Seabees,[66] and temporary trailers like one would find on a civilian construction site. Living quarters, bathroom trailers, and working spaces were virtually adjacent, which with the exception of trips to the Marine chow hall, made for a compact and virtually complete world for SOTF personnel which promoted insulation. The headquarters consisted of several interconnected tents that housed offices, a tactical operations center, an intelligence "fusion" center, and a conference room for briefings and video-teleconferencing. Most personnel worked on phones and laptop computers, usually several at each desk to access

[66] Construction Battalion (CB or "Seabees") is the Navy's combat engineering corps.

different classified networks (Figure 5-10).[67] While the popular conception of a special operations command center is of a buzzing hub of activity, the normal atmosphere pervading the SOTF was one of administrative routine, even boredom.

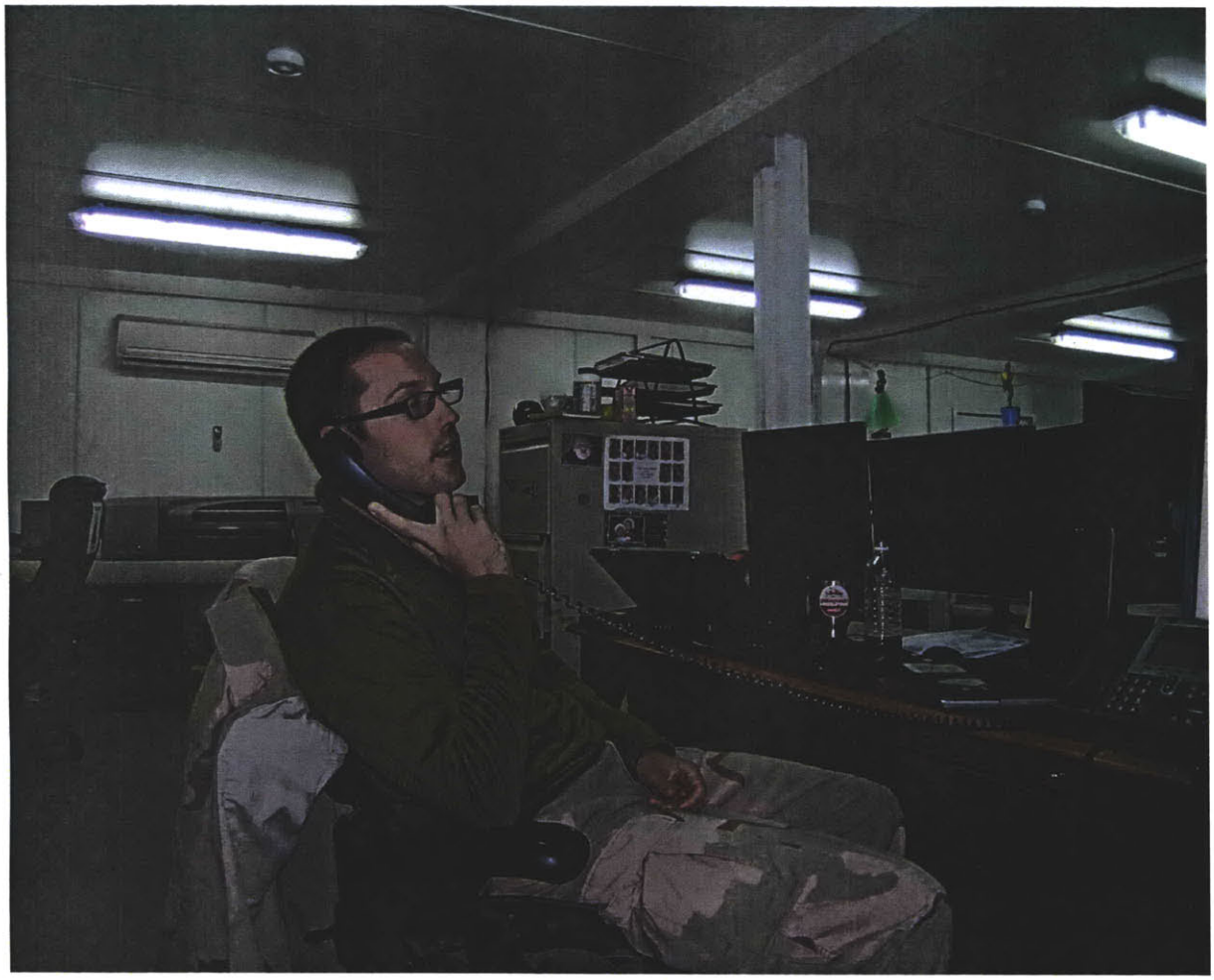


Figure 5-10: The modern staff officer at war (Author's photo)

A great deal of "battlefield circulation" was undertaken for predominantly informational purposes. Not only did digital communication not replace travel, it increased the demand for it. First, IT made travel easier by facilitating more efficient airspace and passenger management.[68] Second, and more importantly, the pragmatic context of use made information meaningful, and

[67] Some added additional monitors to view multiple windows at a time, and if lacking these, users tended to cycle through the multiple windows open at any time.

[68] Schedule changes and delays could be propagated throughout the system and passengers could arrange long distance itineraries on short notice. Routine air travel, with its regular and stable ontology of airfields, aircraft, flight routes, cargo, and passengers, was improved through enterprise integration of IT.

that context was not readily transmitted digitally. The daily routines, conversations, and interactions with tools that weren't explicitly recorded were critical for understanding what role specific representations played in a unit's operations. Digital networks provide translucence not transparency: communications advertised that there was even more to see in person. High levels of email, telephone, and video-teleconference communication did not obviate face-to-face communication, put rather made it indispensable in order to make sense of the former. Action officers sought personal contact with counterparts up and down the chain of command in order to orient to and influence one another's intentions. On-the-ground situational awareness—regularly sought by commanders and their staff—suggested questions and answers that just wouldn't apparent from virtual interactions alone. Digital communication was complementary to travel in person, rather than a substitute, because of persistent information asymmetries throughout the organization.

At the same time, the headquarters routine of meetings, email, access to local systems, and casual conversation constituted a rich situated context all its own. Staff members who took trips to gain situational awareness at another site risked losing it at the SOTF headquarters. Those who traveled too much were often out of the loop in current plans and events (and could be accused of indulging in "war tourism") while those who didn't travel enough could be lulled into the illusion that reality was adequately represented through email and *PowerPoint*. This risk would be mitigated somewhat if the desk-bound staff officer could empathize with the distant interlocutor by virtue of having lived his job in a previous assignment. Both travel and shared experience contributed to constructing the rich context needed on both ends to bind the representational activity at the SOTF to its operations in the field.

Hardly a static collection of people and tasks, the SOTF was a hub in an active circulatory system of people and information. There was a constant flow of visitors to the SOTF from both subordinate and external organizations: staff from tactical and operational higher headquarters, television and newspaper reporters, contractors delivering or repairing gear, members of the relieving squadron starting an early turnover, political delegations and senior military leadership looking for "news from the front," Marines from the divisional headquarters, *etc.* Some of these visits made little impact while others were major evolutions involving camp "field days" and "dog and pony shows." Some lasted only a few hours, others days or weeks

(during which the visitor wandered around nomadically looking for open computers, or was stashed out of the way on a free machine). Likewise SOTF staff members often took trips to visit the Task Units or the CJSOTF higher headquarters. The SOTF's air operations shop spent the majority of its effort simply coordinating the routine movement of all these travelers.

5.3.3.3 Behind the Green Door

The SOTF, like most military units, operated in a classified information environment. Information, far from being virtual or weightless, was protected by an elaborate physical infrastructure of bases, barbed wire, and controlled entry (Figure 5-11). Gaining access to information required overcoming the physical and organizational barriers that partitioned information networks.

Figure 5-11: Concrete T-walls and barbed wire protect a SCIF (Author's photo)

U.S. classification guidance includes levels of classification, handling caveats, releasability and declassification instructions, and a parallel system of sensitive compartmented

information (SCI) which can only be handled within specially accredited SCI facilities (SCIFs).[69] Physically separated (or "air-gapped") internetworks at each level featured a working environment that would be familiar to most contemporary computer users (Microsoft *Windows* and *Office* software, browsers, websites, email, *etc.*), but each was administered by a different bureaucracy with inconsistent offerings of applications, updates, and technical support. Staff members thus had to have multiple non-interconnected machines on the same desk to work across these networks.[70] Users had to remember which network they were typing into so as to avoid inadvertent "spillage" of classified information to an unaccredited network. Spillage events could trigger investigations and reactions by security managers to shut down entire websites, which was sometimes justified to contain valuable information but sometimes just work-slowing overreaction.

Chapter 6 will further describe some of the friction-creating consequences of classification practices. I mention them here only because deliberate fragmentation of information systems in the name of information security is a fact of military and intelligence life. A degree of internal disensus is thus built into the system in order to protect sources and methods.

5.3.3.4 Fragmented Organizational Networks

Every computer network must be managed by some organization. Even when networks of the same classification are technically connected, it may not be easy to move information across them. An internet is a network of networks, so while in principle it should be possible to reach a connected network from any other because they all share the same protocols, in practice connectivity was constrained by the properties of the sub-networks.

The SOTF's working network was the Secure Internet Protocol Router Network (SIPRNET), but there were multiple networks that actually comprised it. The SOTF used

---

[69] U.S. Executive Order 12958, Classified National Security Information, as amended by Executive Order 13292 (March 28, 2003), http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html. Activities within a SCIF are often referred to as happening "Behind the Green Door," a reference to a 1972 pornographic movie of the same name. This reference appears lost on many young personnel who use the expression nonetheless: it's not uncommon to hear earnest opinions to the effect that "SCIF doors were painted green in Vietnam."

[70] A workstation in a SCIF might have three or four separate computers. A user could interface with these machines through multiple monitors and keyboards dedicated to each computer, or each could be connected through a junction box to a single monitor and keyboard, allowing the user to interact with each computer in serial.

different SIPRNET networks: SOCOM's Tactical Local Area Network (TACLAN), and a Marine SIPRNET network. Each of the SOTF's locations accessed TACLAN via a hardware suite designed to be deployed and set up quickly to provide a local file-sharing and access to SIPRNET through a satellite link (SATCOM). The topology of the network was such that a unit's internal TACLAN communications were routed through local servers, but email or web access between units or to the broader SIPRNET was routed through SATCOM via the continental U.S. and back. Thus a TACLAN email sent from the SOTF to its Task Unit across the parking lot or to the Marine headquarters one kilometer away was routed via SATCOM to the U.S. and back. The Marine network was far more robust by comparison, with high-bandwidth local connections between bases providing access to file and web servers. The Marines hosted a very large website with a wealth of useful information including insurgent databases, daily intelligence updates, operational plans, and a vast amount of other information critical to SOTF operations. Large multi-megabyte *PowerPoint* files could be transferred relatively quickly over the Marine network, but were achingly slow to download via TACLAN and subject to network timeouts that could prevent downloads altogether.

These two different networks reflected two different concepts of operation and different chains of command. TACLAN was designed to provide a small SOF unit with autonomous capability and connectivity back to home base. The Marine network was the evolutionary product of large scale occupation of the same bases in Iraq year after year since 2004. This difference was even reflected in the types of computers in use, with the SOTF fielding small laptops while at the Marine headquarters, desktop machines and larger monitors that were more ergonomically appropriate for a long deployment were prevalent. The SOTF conducted the bulk of its business over its own TACLAN, including communications with the Marines. In the SOTF HQ at the time there were only three computers connected to the Marine network, two for intelligence and one for the legal officer (JAG), which had been acquired on an informal handshake between an officer at the SOTF and an officer in the Marine's intelligence systems division. These three machines provided access to a wealth of information on Marine file servers that was not posted on the Marine webpage. To move data from a SOTF machine to the Marine machine right next to it on the same desk required using email (routed via the U.S.) or

contraband removable media.[71] The email servers of the two networks did not share address books, which made it difficult to find people across them. Internet connectivity by itself was thus not enough to enable easy information sharing: technical and organizational topologies still created barriers to accessing information, even when everyone was cleared to see it and ostensibly working together.

Within the SOTF organization, distributed basing also fragmented networks. Each Task Unit and Det ran its own local TACLAN, so SOTF visitors to each site had to obtain local accounts to access the systems.[72] Intra-SOTF travelers ended up with multiple email accounts at each of the operating locations, where emails would be marooned when they left. Access to networked data was still very dependent on physical access points.

Voice networks were also segmented by classification and organization. SOCOM communication used one voice-over-IP (VOIP) network, while conventional forces throughout Iraq used a different Secret VOIP (S-VOIP). Unlike the case of data, where the SOTF relied mainly on the SOCOM TACLAN, most SOTF voice was carried over the S-VOIP provided through the Marine SIPRNET (another dependence of SOF on the Marines). Unfortunately S-VOIP access outside of the CENTCOM theater was extremely limited. The advantage of S-VOIP was that, since it rode the encrypted SIPRNET, users could directly dial calls and discuss classified information openly and clearly; by contrast, older switched networks (DSN) required users to initiate encryption using controlled key material and secure telephone units (STUs) which tended to garble voices and drop calls. The theater organization was thus a generation of technology ahead of many organizations in the U.S., but the theater S-VOIP was not compatible with the previous generation of STUs, which degraded connectivity with support organizations in the US. This effectively disabled most secure voice communication between the SOTF and reach-back intelligence support at organizations like the Office of Naval Intelligence and the

[71] One innovative user rigged USB cables from each machine to another cable on the desk to a removable hard drive, making it easy to switch the cabling right at the desk.

[72] While it was technically possible to use the same email address on these different networks, this was complicated by the SATCOM bandwidth issues mentioned above and by variable technical know-how regarding remote connections.

NSW Mission Support Center, forcing recourse to written email.[73] Incompatibility between IT "stovepipes" has persisted for decades since first flagged as a major problem.

5.3.4 Hypotheses on Internal Consensus

Table 4-5 summarizes the foregoing discussion in terms of the hypotheses about internal consensus from the last chapter.

Table 5-4: Hypotheses on SOTF internal consensus and information friction (IC→IF)

Internal Consensus	Value for Anbar, Iraq	Effect on information friction
IC11. Doctrinal preferences	SOF prefers direct action; Marines in Anbar prefer indirect action	↑ (Coordination with Marines) ↓ (SOTF internal)
IC12. Number of actors	Many, diverse, and changing	↑
IC13. Autonomy	SOF chain of command; tenancy in Marine battlespace	↑ (Tactical coordination) ↓ (SOTF mission emphasis)
IC14. Division of labor	Controversy with Marines over SOF role; internal confusion with last-minute SOTF augmentation	↑
IC15. Definition of protocols	Many, fragmented networks	↑
IC16. Complexity management	High agency & transaction costs	↑
IC17. Semantic interoperability	"Stovepipes," constant battlefield circulation required	↑
IC18. Investment	Most dangerous, most risky scenario (not indirect action)	↑
IC19. Adjustment	Tedious coordination; ingrained SOF worldview protected by secrecy and autonomy	↑
IC20. Accountability	Abundant records of transactions, disorganized in local files	↑ (work-to-rule, personalization) ↓ (investigations feasible)
Net Effect	**Significant Political Complexity, with SOF doctrinal consensus amid external instability**	**Decentralized Interference & Doctrinal Insulation**

The net effect of the situation in Anbar is to raise information friction. This is a little more nuanced, however, in that one component of internal consensus, doctrinal agreement, is extremely high in the case of SOF direct action. This would tend to lower information friction

[73] Email, in turn, often took too much effort to communicate in sufficient detail and contributed to the isolation of reach-back from operational reality. The only voice alternatives were unencrypted DSN, which tempted conversants to "talk around" classified material in the clear (a dangerous practice that hostile intelligence can exploit), or another SCI network which was not widely available. There was an additional VOIP alternative available in an NSW-specific instant-messaging application called "Webbe," but as this application was not on any official Navy or Defense list of approved applications, ONI's IT managers would not permit its installation there.

except when the consensus is misaligned with the unstable external environment. Thus the net effect is of overwhelming interference between and within organizations, but also with some insulation of doctrinal worldview within the SOTF.

5.4 Haphazard Adaptation

The third condition for reliable information systems is an organizational capacity to actively address information friction in the course of actual operations. While expedient adaptation is the only emollient that can relieve information friction once war is underway, nevertheless, decentralized adaptation inherently risks creating interference friction for the larger system. Open technology, low barriers to technical expertise in forward locations, and institutional support for user innovation all improve the odds that bottom-up adjustments will lower information friction, but the SOTF did not have all of these components of expedient adaptation. The ubiquitous Microsoft *Office* environment provided the SOTF with a set of powerful tools for bottom-up adaptation, and the improvisational, meritocratic culture of SOF provided latitude for personnel to use it. However, technical expertise was very unevenly distributed or misapplied, so local expedients created many negative externalities. The following chapters will provide many examples. SOTF personnel were able to adjust their information system on the fly to deal with information friction, but a lot of that friction was actually the consequence of similar such adjustments. The net effect on information friction here is ambiguous, as friction-lowering measures have much potential for self-inflicted friction.

5.4.1 Information Processing as Indirect Work

One might reasonably expect that an organization would be pretty good at a mission it likes to do, especially one with the autonomy and funding of a SOF outfit. The organization prefers to conduct commando exploits, but the informational work that is needed to support it is *not* something that it likes to do. Symbolic representations of the world—the stuff of staff work and intelligence—are inherently an indirect way of dealing with the world. Indirect, symbolic, informational work does not accord well with a commando identity. Of course, it is important not to conflate representational indirection, which is about dealing with information, with SOF indirect action, which is about dealing with indigenous people. Yet they do have something in common, in that they both involve negotiating agreements with others and managing relationships between organizations. In the case of training and engagement, indigenous

alliances are critical. In the case of information work, relationships among machines, people, and organizations are very important. Like relationship-building with locals, information work generally lacks immediate gratification; it's complex and hard, with ambiguous feedback. Both information work and indirect action are at odds with the basic commando identity of SOF organizations. The difference is that personnel involved in direct-action information processing can at least vicariously participate in direct action. Information processing in support of indirect action should be doubly neglected.

5.4.1.1 Analog Frogmen

SOF culture has an ambivalent relationship to technology. On the one hand it is an early adopter of the latest gadgets, generally having more advanced technology than comparable conventional units, and SOF aggressively seeks to employ technology throughout the enterprise. On the other, it is normal for SOF operators to brag that "I don't really get along with computers" or "I'm just an analog frogman." This attitude comes to be shared by support specialties which look up to higher-status operators, such that even information-intensive support fields like intelligence will tolerate mediocre ability with information tools. A marginalization of information skills helps to make the social scaffolding of technological infrastructure work more invisible, and perpetuates reliance on buying new gadgets to make computation easier.

Whereas operators are obsessive about their weapons and other operational kit, looking to customize and master their employment in field conditions, this technological enthusiasm generally does not extend to computer applications. All technology is not culturally equivalent: while high-tech weapons and operational kit enhance the elite warrior image cultivated by SOF communities, IT proficiency would promote a geekier image. It is inconceivable that an operator would ever say "I really don't like guns," yet when they fight a war through a computer screen, as staff officers must, many proudly make a point of not being very good at using a computer. While weapons technology is exciting, information technology is merely necessary. Clearly, no operator ever joined the Green Berets or SEALs to work behind a computer, but nevertheless, this derisive (and infectious) attitude toward information skills is ironic given the heightened dependence of modern warfare upon them.

5.4.1.2 Second-Class Citizens

Well over half of the Naval Special Warfare (NSW) community is composed of non-operator support personnel, whom "operators" refer to as "techs" with a slightly pejorative connotation.[74] While this is consistent with the normal tendency of troops exposed to greater danger or matriculated through more arduous training regimes to look down on support personnel "in the rear with the gear," it is particularly pronounced in NSW. The second-class status of support personnel even extends to military specialties that accompany SEALs on missions in the field, such as explosive ordinance disposal (EOD) and tactical cryptologic technicians ("ears on target"), who are exposed to similar risks (or sometimes greater, in the case of EOD) but are not themselves elite "shooters." The larger SOCOM community also makes an "enabler" vs. "SOF" distinction, but it is neither as severe nor as exclusionary as in NSW.[75]

Overall the NSW community is mission-focused and meritocratic, like SOF in general, so SEALs do value competence and initiative over rank or position. This ethos does indeed extend to support personnel who are good at what they do. Compared to other Navy communities, NSW has an encouraging, upbeat, and informal environment which welcomes competent help. Nevertheless, even skilled support personnel remain outsiders to the brotherhood. A "tech" vs. "operator" caste system is one of the defining features of NSW culture. The attitude is partially reinforced by "techs" themselves who live vicariously through SEAL operations and hope a little prestige will rub off. The worst offenders seek out tactical training, weapons, equipment, or relaxed grooming standards in order to promote an unearned "operator" image, and SEALs understandably resent the sycophancy.[76] Not all of the professionals on which SEALs depend behave that way, however, but they unfortunately get marginalized as well. SEALs are brought up to believe that a frogman can and must be able to do anything himself. A task element could end up far behind enemy lines or far from support, where SEALs would have to improvise and

---

[74] The NSW community in 2007 consisted altogether of about 6,700 personnel including 2,300 SEALs and 600 Special Warfare Combat Crewmen (SWCC "boat guys" are still "operators" but with less prestige than SEALs); Scott R. Gourley, "NAVSPECWARCOM Year in Review," *The Year in Special Operations* (2008), 59-65.

[75] One reason is that land warfare is an anomaly in "big Navy," and most support personnel only visit NSW for a single tour of a few years. Army-dominated SOCOM, by contrast, is composed of personnel who are all basic soldiers in addition to their branch specialties, and so joining a SOF unit is not so extreme a change. For a sanguine view of SOCOM's elite culture see Jessica Glicken Turnley, "Retaining a Precarious Value as Special Operations Go Mainstream," Joint Special Operations University Report 08-2 (2008).

[76] The NSW Center (which runs BUD/S) regularly has to verify whether individuals claiming to have been Navy SEALs have in fact graduated from BUD/S or are just masquerading as SEALs.

provision themselves in order to survive. Thus support personnel come to be seen less as complementary professionals and more as servants taking care of work that frogmen could do just as well or better if they weren't so busy being commandos. Unfortunately SEAL training prepares them not at all for the ubiquitous challenges of knowledge work in modern warfare.

The "tech" population increasingly includes intelligence and IT support because SEALs, like other military communities, have become thoroughly dependent on information in the past decade. Four separate and imperfectly coordinated attempts to institutionalize NSW intelligence provision resulted in haphazard offerings of expertise.[77] Many support personnel are not integrated into NSW organizations until just prior to deployment, and as discussed above, there is little consideration given to their competence to manage both the content and format of complex information systems. Technical IT and intelligence expertise is the luck of the draw.

5.4.2 Network Managers Uninterested in Information Content

Knowledge-management expertise was not abundant in the IT department, the SOTF's "N6" or "C4I" staff section. IT network managers have a full-time and unforgiving job in any firm because they have to deal with uneven user adherence to policy, frequent software upgrades from multiple vendors, and angry demands to maintain service.[78] For the military the job is furthermore complicated by dust, weather, wartime stress, spare parts limitations, personnel turnover, SOCOM and Navy information security and configuration policies, and the vagaries of enlisted information technician quality and training.[79] N6 was responsible for the TACLAN

---

[77] The four components are: (1) intelligence personnel from the Navy's larger intelligence community; (2) a "reachback" Mission Support Center in Coronado; (3) dedicated support from the Office of Naval Intelligence John F. Kennedy Irregular Warfare Center, nee "Trident," which fields Tactical Intelligence Support Teams; (4) NSW Support Activities (SUPPACT) which have been nurturing organic HUMINT, SIGINT, and IMINT capabilities. In 2006 Naval Special Warfare Command converted congressional appropriations it had received for two additional SEAL Teams into the creation of the SUPPACT concept on each coast. These units would field deployable Cross Functional Teams providing advanced special operations, tactical information operations, and technical special reconnaissance. The concept was still embryonic and haphazardly integrated in 2007, and in any case was totally co-opted by the focus on direct action as little more than a target-generation capability. On the SUPPACT concept see Scott R. Gourley, "NAVSPECWARCOM Year in Review," *The Year in Special Operations* (2007), 148-155; Couch, *Sheriff of Ramadi*, 40-41, 219-222.

[78] Indira R. Guzman, Kathryn Stam, Shaveta Hans and Carole Angolano, "Human Factors in Security: The Role of Information Security Professionals Within Organizations," in *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions*, ed. Kenneth J. Knapp (Hershey, NY: Information Science Reference, 2009), 184-200.

[79] Interestingly, IT support staffs in theater seemed more supportive than those in military and intelligence organizations in garrison. The former appeared more willing to work with users and support their mission as expediently as possible, while the latter emphasized protecting system security and complying with policy over the

SIPRNET which carried the bulk of daily operational traffic, two different unclassified networks, the Marine SIPRNET connections, radio and telephone voice networks, and the top secret JWICS network. When SOTF systems went down because of a software fault or loss of generator power or air conditioning in the blazing summer, staff work would slow considerably.

As long as computer and communication networks were up and running, N6 personnel were agnostic about the meaning of information for operations. However, significant overlap often emerged between IT service and content. Staff members interested in content matters often found themselves embroiled in technical details when they needed to connect to particular networks, configure applications, or procure some specialized software or equipment. Interactions could become testy if the staff member in question happened to have some computer expertise compared to the technicians with the actual authority to make changes. Because the NSW squadron was composed of several different components, many users would show up on deployment with their own computer hardware and software which they expected to plug into the network. This was especially true of the information-intensive enablers such as the augmenting intelligence teams which had independent budgets for top-of-the-line gear but did not deploy any IT support of their own. They expected N6 to make it work on SOTF networks and to help keep it running, even though N6 had never seen it before.

5.4.3 Strong Improvisational Ethos

The SOF community has a strong improvisational ethic: get the mission accomplished, with whatever you have available. The classic scenarios include a Special Forces team working to coddle an indigenous warlord in a remote area, or a team of commandos deep in enemy territory with little support. The SEAL community, furthermore, was utterly neglected by the Navy for most of its history before SOCOM stood up, so it built up a strong ethos of making due with available resources. Organizational autonomy, discretionary resources, and leadership encouragement of innovative thinking promote low-level expedient design. SOF will beg, borrow, or steal what they need and cobble together a working solution.

---

effect on productivity. At one point an individual who had redeployed back to the U.S. called back for computer support to the Marine IT shop in Fallujah because the IT department at ONI was unable to help her. orward technicians were closer to operational users in a wartime environment, and thus were more motivated to streamline bureaucratic requirements to meet mission needs, whereas technicians in the rear adhered more rigidly to existing policy.

The major caveat to this sanguine story, as discussed above in the marginalization of "techs" and the administrative focus of network managers, is the neglect of IT expertise in forward areas. Thus improvised knowledge management solutions are liable to be rife with scalability, interoperability, and reliability concerns. SOF networks are loaded with powerful software tools that enable expedient adaptation, but their organizations are not so flush with personnel who know how to use them most effectively.

5.4.4 Hypotheses on Expedient Adaptation

Table 4-6 summarizes this discussion in terms of the expedient adaptation hypotheses from the last chapter.

Table 5-5: Hypotheses on SOTF expedient adaptation capacity and information friction (EA→IF)

Expedient Adaptation	Value for Anbar, Iraq	Effect on information friction
EA1. Extensibility	Flexible Microsoft Windows/Office software	↓
EA2. Licensing	Some proprietary software, ubiquitous MS Office	↑↓
EA3. Discretionary resources	SOF discretionary money & resources provides slack	↓
EA4. Location of technical expertise	Limited to network admin & opportunistic skills	↑
EA5. Novel designs	Rampant informal prototyping	↓
EA6. Boundary-spanning figures	Situation-dependent, SOF isolated from Marines, frequent circulation	↑↓
EA7. Technical literacy	Variable quality, technophobic	↑
EA8. User community	Collegial exchange of ideas & prototypes, but with high situational barriers to transmission	↑↓
EA9. Practical ethnography	Attention to representational practices, personality dependent	↑↓
EA10. User innovation support	SOF enables & reward initiative, experimentation, communities	↓
EA11. Organizational retention	Reinvent solutions each deployment, subject to favorite pet projects of superior HQs	↑
EA12. Externalities	Users unmindful of positive & negative externalities	↑
Net Effect	**Flexible tools without expertise**	**Ambiguous; Interference**

I have not yet discussed everything summarized in the table because I will describe actual usage patterns in far more depth with examples in the following chapters. The point here is that

the components of expedient adaptation combine for a quite ambiguous overall effect. Flexible tools and SOF culture promote improvisational adaptation, but the marginalization of IT and intelligence expertise introduces barriers to technical expertise. Thus we should expect to see expedient adaptations that lower information friction in proscribed situations, but which also raise information friction across settings because of heightened risk of negative externalities.

5.5 Expect High Information Friction

The strategic and organizational context of operations in Anbar, before we even get too deep into the SOTF's human-computer interactions, exert conflicting pressures on the SOTF's information systems, with a net tendency toward high information friction. To sum up, we should expect a lot of interference to be manifest because of the ontological complexity of irregular warfare, abundance of counterinsurgent actors in Anbar, and noisy information practices within the SOTF; some enterprise integration in the systems supporting direct action; and an insulated obsession with direct action targeting because the strong preferences and autonomy of SOF were misaligned with the counterinsurgency realities in Anbar. As emphasized repeatedly in this project, the end result of IT usage for any given information system is somewhat indeterminate and quite dependent on context. Advanced IT alone does not a revolution make. Particularly strong cultures in particularly complex environments can generate quite dysfunctional information systems. The next chapters turn to the way people actually used IT in the SOTF, first describing general interference in the daily use of digital IT, and then describing insulation of IT usage to support direct action targeting.

Chapter 6: Interference Patterns

> "Improvements in communication...make for increased difficulties of understanding." –Harold Innis[1]

6.1 The Administration of Violence

The previous chapter introduced a U.S. special operations task force (SOTF) in Iraq in 2007-2008. The SOTF was built around a core SEAL Team with various last-minute Navy and Army augmentation, all operating on a complex battlefield full of many other military, civilian, and Iraqi actors. Operations required personnel to work through relationships with indigenous actors, bureaucratic colleagues, and technological equipment, which are all "indirect" activities at odds with strong doctrinal preferences for commando "direct action." The values of internal consensus and expedient adaptation, two of the three causes of information friction, are mixed in this case; nevertheless, along with clear external instability, they altogether lead us to expect high information friction. This chapter and the next will show how it was high indeed.

Daily interaction with information technology (IT) like email and *PowerPoint* fostered endemic coordination problems, the interference variety of information friction. However, even though representational practice was obtrusive and time-consuming for "operators" and "techs" alike, it was also somewhat invisible within a culture constructed around more dramatic exploits. The chapter after this will draw out the insulation variant of friction.

If some of my data on everyday IT employment seems to emphasize the mundane or trivial, then that's because a lot of contemporary military effort seems to be absorbed in trivialities. For all its life and death consequence, information age war with its increasing proportion of personnel in knowledge work recreates the quotidian frustrations of office life anywhere. One review of the sociology of scientific knowledge sums up "the thrust of a great deal of work...as concerned to show in concrete detail the ways in which the making, maintaining, and modification of scientific knowledge is a local and a mundane affair."[2] So too do military personnel spend their time, as Clausewitz puts it, with "endless minor obstacles" rather than "great, momentous questions," and now more than ever in an information-intensive

[1]Harold A. Innis, *The Bias of Communication* (Toronto: University of Toronto, 1951), p. 28

[2] Steven Shapin, "Here and Everywhere: Sociology of Scientific Knowledge," *Annual Review of Sociology* vol. 21 (1995): 289-32

milieu.[3] The juxtaposition of office space follies with the use of lethal force can seem profoundly uncanny and more than a little discomfiting. Indeed, one unintended consequence of the information revolution for the conduct of war is that personnel can become so preoccupied with the irritations of incompatible software, so invested in emotional spats over information access, and so seduced by the neat packaging of the battlefield on *PowerPoint* slides, that the conduct of war itself can become trivialized. Given dramatic popular images of high-tech warfare, this should be surprising. Given popular frustration with everyday high-tech systems, however, this should not. When attention becomes distracted from the bloody business at hand, then it's more likely that power will be used irresponsibly.[4]

Sections of this chapter will seem rather discursive to some readers. This ethnographic data about military IT hasn't been documented elsewhere, so I've taken some space to do so here. The chapter after this one will more directly take on the performance implications of all this activity.

6.2 Cognitive Prosthetics in the Task Force

Many of the SOTF's representational tools would be familiar to Microsoft *Office* users anywhere. The headaches of digital administration are largely consistent with studies of IT usage in corporate or academic environments, as per the theme of civilianization raised in Chapter 2. There were some differences in this peculiar environment, which I will highlight along the way. I will discuss the major genres of representation at the SOTF with the important exception of social network diagrams, which I will defer until the next chapter because they figure so centrally in the targeting problem.

All of these tools were used to facilitate perception and to make it more reliable. However, usage regularly drifted into episodes of friction where information format became obtrusive and content thus unreliable or unavailable. User phenomenology (participants'

---

[3] Carl von Clausewitz, *On War*, trans. and ed. Michael Howard and Peter Paret. Princeton (NJ: Princeton University Press, 1976), 120

[4] I am not making the same argument as Hannah Arendt, *Eichmann in Jerusalem: A Report on the Banality of Evil* (New York, NY: Viking Press, 1963), not exactly anyway. The military blunders which flow from information friction are tragic rather than evil. Except for unfortunate cases of atrocity like the My Lai massacre, U.S. military personnel usually uphold impressive standards of honor and integrity. Yet personnel can be distracted, and their attention displaced to unproductive or counterproductive targets, even with the best of intentions. There is indeed a certain banality in the conduct of modern American warfare, but it is not evil.

experience with tools) and cognitive functionality (aspects of tools that reveal features of the world available while masking others) waivered unstably between regimes of low and high friction. In these recurrent episodes of obtrusive information format and unreliable content, the tools constantly got in the way of attention to the mission, and of course it was only through the tools that the mission could be perceived at all. As a result, staff officers were preoccupied with debugging representational processes along well-worn paths, rather than taking in the view which tools afforded and trying to make sense of their options in world. The flexibility of the tools allowed them to make local changes to facilitate their own sensemaking, but for the same reason they tended to undercontribute to public goods like organized files and common data management schemes, thus generating more friction. Expedient adaptation undertaken to work through friction here became a source of friction as well.

6.2.1 The Persistence of Paper

Automation has not banished paper, and has if anything increased its consumption. Trigger-happy on the print button, SOTF personnel burned through reams of paper and boxes of toner cartridges. The practical implications are (1) information that is written on or arranged with paper tends to be locally situated and not necessarily communicable over digital networks, and (2) personnel use paper to supplement and enable their interaction with digital representations. Digital data is an imperfect substitute for paper, and paper seems to be an important complement.

6.2.1.1 Advantages of Paper

Paper has some affordances that digital representations don't have.[5] One can comfortably read its high resolution print in ambient light, adjusting the distance to the eye. Multiple pages can be thumbed through quickly while preserving a sense of overall structure. Not tethered to monitors, paper can be taken to other locations to read, mark or discuss, either in private away from curious coworkers, or in meetings with them away from computers. One can exploit the spatial layout of text when annotating and make gestural markings like circles and underlines. It can be posted on a wall for easy reference, crudely sorted into piles on a desk, or arranged in binders. The very physicality of paper preserves a history of interactions with it, which is useful for maintaining a "master" working document, or for collecting a series of

[5]Abigail J. Sellen and Richard H. R. Harper, *The Myth of the Paperless Office* (Cambridge, MA: MIT Press, 2003)

approval signatures or certifying stamps. It also provides some durability: as one SEAL observed, when you shoot a paper notebook you have a notebook with a hole in it, but when you shoot a laptop computer you have a pile of junk.[6] Many complementary uses for paper persist even when digital media substitute for others. The embodiment of paper contributes to its usefulness above and beyond the information "on" it.

6.2.1.2 Varieties of Printouts

Many printouts were produced for temporary uses. People often printed digital documents in order to exploit the interface affordances of paper (readability, portability, annotation, *etc.*) and then disposed of it not long after (stuffing paper into "burn bags," grocery sacks that were literally tossed onto a campfire at the SOTF every few days to destroy classified waste). Other printouts ended up on the wall indefinitely, displaying the location of subordinate units and geographic features, tribal boundaries, command guidance, networks of insurgents, *etc.* These tended to accumulate annotations, pins, sticky notes, and other updates as time went on, leading to a divergence between digital and paper versions that personnel tended to delay reintegrating. Office denizens used these paper products not only by for reference but also as impromptu briefing aids for the regular stream of visitors circulating through the SOTF.

Another type of paper printout was incorporated into various bureaucratic genres—signed evaluations, stamped orders, routed approval forms, *etc.*—to signal official validation. In these cases paper combined with signatures, stamps, or seals were used to preserve higher barriers to reproduction and hence to preserve the validity of the bureaucratic signal. These forms carried physical traces of their encounters with officialdom (stamps and signatures), providing some slight protection against forgery that didn't come as naturally with digital media. Some of these would be physically archived for long-term storage, as the physical trace was itself an important piece of information. That trace could be used to argue a bureaucratic position, to get paid, or for protection in an investigation.

6.2.1.3 Handwritten Notes

Other paper representations did not start off digital at all. Yellow sticky notes were attached to monitors, desks, and other pieces of paper. Small green bound notebooks jammed

[6] Fair enough, but if you don't shoot the laptop, then you have a wealth of other software tools that paper can't provide. This quip is an instance of the aforementioned SOF ambivalence toward technology: weapons are awesome, IT is lame.

with various slips of paper were ubiquitous, recording phone numbers, meeting notes, to-do lists, and other jottings. My field notes for this ethnography started off as work-relevant jottings in such notebooks. When personnel reached the end of their notebooks, they often took some time to go through them and manually transfer data into a new notebook, rewriting commonly used phone numbers and passwords into the cover. Because such information was never digitized, it was usually quite local to its embodiment.

6.2.1.4 Whiteboards

Whiteboards provided another physical medium for writing in SOTF spaces. They were mainly used to facilitate freeform conversations among staff officers working on a problem, who used graphical gestures and made lists.[7] Information tended to remain on a whiteboard until someone else needed to use it, leaving traces of old conversations that appeared quite puzzling to subsequent observers, who were often reticent to erase the residue.

In an earlier and less electronic SOTF environment, whiteboards would have been used to track upcoming and ongoing missions, flights, or projects. The physical whiteboard provided a public, synoptic, coordinating role allowing important items and their relationships to one another to be seen all at once by multiple people as the information was updated (*i.e.*, what is the approval status of those missions, who is tasked to do what, what are the communication frequencies and codewords, which flights are delayed, *etc*). For such uses, the working storage of the whiteboard was simultaneously its display. By and large this whiteboard application had been transferred to digital spreadsheets, breaking the link between storage and display. While digital spreadsheets could accommodate more data, provide more analytical and formatting power, facilitate communication of data to others not at the same site, and could easily be backed up, the positive by-products of the large format whiteboard were sacrificed when users had to peer through the small window of a single monitor. The large-format aspect of the whiteboard was, ironically enough, recreated in some cases—such as mission and flight tracking—by dedicating a projector and a computer to continually cast an image of the spreadsheet on the wall. The embodiment of the representation played a role above and beyond the narrow content of what was stored, and this role had to be rediscovered and recreated once it was lost in

[7] This happens more or less in the way scientists develop and coordinate shared concepts, as described by Lucy A. Suchman, "Representing Practice in Cognitive Science," in *Representation in Scientific Practice*, ed. Michael Lynch and Steve Woolgar (Cambridge, MA: MIT Press, 1990), 301-322.

translation from whiteboard to spreadsheet.[8] The separation of storage and display bought more capacity and flexibility at the price of more complexity in having to manage and maintain more technology to do these different roles (and both were dependent on electricity, unlike the whiteboard and paper).

In notebooks, whiteboards, and printouts, much meaningful information in the SOTF was not stored on computer servers at all. It persisted in handwritten comments, little green notebooks, in the spatial arrangement and bureaucratic history of paper on desks and files, and in the performative functions of wall charts and paper officialdom.

6.2.2 "It's on the Share Drive"

The SOTF stored most of its digital information on a networked file server or "share drive." It was generally accessible by any user on the local network, but the N6 could set user and group level permissions to restrict access to some folders (thus, interestingly, intelligence was visible to all while personnel data was restricted). The capacity of the share drive was for all practical purposes unlimited because computer memory was relatively inexpensive.[9] The share drive thus grew into an inscrutable labyrinth of folders and files. Tidy files are a public good which personnel could not collectively provide.

6.2.2.1 Accumulation of Files

The share drive contained a vast amount of data. It held over one million files totaling nearly 632 gigabytes (Gb), an average of 1.27 megabytes (Mb) per file. Of all the data on the share drive, 121 thousand new files (12% of the total number) or 167 Gb (26% of the total size) were created during a seven and a half month span. The average daily increase of 526 files (723 Mb) did not vary with the pace of operations or much at all, suggesting that the steady growth was driven by internal organizational factors rather than environmental demand like the irregular fluctuation of direct action missions. If the accumulation were graphed over time (not displayed here), one would see a small number of large step increases (*e.g.*, 20k files totaling 18 Gb at

---

[8] Edwin Hutchins, "How a Cockpit Remembers Its Speeds," *Cognitive Science* vol. 19, no. 3 (1995): 265-288 describes how, in the transition from analog to digital speed indicators, pilots lost information that they were using in the physical orientation of the arms of the analog dials. The point is not that this loss is an inherent property of digital media, but that there was a fault of design that did not recognize there was additional tacit information in the analog dial which *could have been* retained in a digital representation by paying attention to how the representation was *actually used* to coordinate behavior.

[9] Although only a few years previously, military users would have been regularly exhorted to keep their folder capacity below a certain level, prompting them to purge files (and destroy corporate memory).

once), which appeared to be the result of someone copying over in batch a large amount of data like several DVDs or the entire contents of another directory. Individual files could be quite large: the average *PowerPoint* file was 2 Mb while the largest was 183 Mb; the average *Outlook* email repository was 513 Mb while the largest was over 2 Gb.

The ease of copying existing files into new locations raises the question of how many of those files were actually new. An indirect way to get at this is to compare the file create date (when an instance of a file is created) and the file modification data (when the content of a file is edited).[10] Only 15% (by number of files and size) of the files added during the deployment were modified after they were created. It appears that the majority of files added were just copies of previously existing files. Of the small fraction of new files, about half of them were last modified only within a day of their creation, meaning that there were not a large number of files which received ongoing edits. Microsoft *Office* files (*Word*, *PowerPoint*, *Excel*, *etc.*) account for most of the files created (58%) and modified (24%), which is unsurprising given these applications are used for most military staff work.

Another way to measure how many copies were strewn across the file server is to compare file names. 117 thousand individual filenames were duplicated at least twice; 3,400 at least ten times; over 300 filenames a hundred times; 30 filenames were each duplicated over 2,000 times; and 3 filenames showed up 26,400 times! Of the total million files on the server, therefore, half of these were duplicate files, and more than a quarter was one of a set of ten or more duplicates. Again this is an imperfect measure, as different files could conceivably have the same names, but it does suggest a great amount of file duplication went on in the normal course of work.

6.2.2.2 Multiple Folder Schemes

The share drive was not just a repository of files, of course. It was organized into folders full of files and more folders. Folder recursion provided many ways for personnel to squirrel away data. There were over 78,000 folders on the server. The average folder depth (the number

[10] If a file is copied, then the copy will have a new create date, but the old modification date will carry over. If the file is never subsequently modified, then the modification date will be before the creation date. New files and subsequently modified copies will have a modification date later than the creation date, whereas unmodified copies will have an earlier modification date (regardless of whether the copy is ever opened for read-only viewing). These statistics are for files whose create date fell within the deployment period. Of these, files are considered unmodified if the modification date precedes the create date (and modified otherwise).

of subfolders in which any given file is nested) was 10, with a maximum of 20. The average number of files in a folder was 13, with a maximum of 88,000. The IT department used over 40% of the share drive space, a substantial overhead for making the other 60% available to the rest of the staff (where operations and intelligence were, unsurprisingly, the heaviest users).

These rough statistics do not adequately convey the Byzantine complexity of the shared file system arrangement. The *Windows* file system abstraction is strictly hierarchical, but life is not. The real world can be decomposed into meaningful hierarchies in different ways to support different activities. Operations people track individual missions and so they want to see all orders, intelligence, and supporting documents consolidated under a folder named for the mission. Intelligence people care about insurgent personalities and so they organize intelligence reporting into target folders for each individual, or they might save intelligence data by reporting sources. Multiple missions may target the same individual, or multiple individuals may be targeted in a single mission, so it would be difficult to say that one hierarchical categorization scheme is *a priori* superior to the other. This is just one instance of the general problem of incompatible ontologies, where categories of entities and relationships are used differently.

Because SOTF users had permission to create and name folders on the share drive, they could construct *ad hoc* and often mutually unintelligible hierarchies. Most users used only a small subset of the share drive, such as their user profile, desktop, or a work-center directory. These warrens of data were functional for those who lived in them but virtually inscrutable to others spelunking through the share drive in an attempt to coordinate across staff sections.

Private folder space provided individual users with working space. Rough drafts, sketches, and messy desks are scaffolding that supports intellectual production of any kind. Personal file system space provided the same function for digital work, serving as a buffer where working files and custom folders could be kept ready-to-hand in crafting the real deliverables. In the digital world, the space available for cluttering is vast. Ample working space facilitated new digital production but also amassed a voluminous residue of earlier production.

6.2.2.3 Management Challenges of Common Servers

Organizing the share drive was a commons problem. Every user could take up space, and for the most part none were excluded. Everyone would have benefited from a well organized,

easily navigable, uncluttered network with few duplicate files. Tidy data was a common good requiring every user to contribute effort by understanding and adhering to a common organizational scheme. Yet with more and more users, each interested only in a subset of share drive data and with different representational needs, the effort to maintain common organization exceeded what each user got from it. Defection from interdependent organizational schemes occurred with intentions to rationalize local data in response to new mission requirements or bright ideas. The pollution of the data commons was inadvertent.

Technical fixes like server search engines were of limited utility amid all the duplicated files, divergent versions, and strange naming conventions. Many people instead just asked their colleagues to manually click through their directories for something, and then asked, "Can you email that to me?" When that colleague was absent or transferred, the data might be as good as lost. When data was found via this method, duplicates proliferated. The ever-expanding capacity of shared servers appears to keep this data tragedy from becoming a real tragedy. Despite the constant rate of data accumulation, much of it clutter, there always seemed to be enough room to accommodate the active working clutter that personnel actually knew how to work with. The active subset of data was just the tip of the iceberg of stored data, kept afloat by ever-expanding memory capacity.

Workcenter supervisors or the SOTF's executive officer sometimes tried to specify file and folder naming conventions in an attempt to enforce enterprise integration. Yet with plentiful server space and open permissions it remained easy for individual users to alter their own folders and files and difficult for managers to monitor and enforce compliance. For instance, one group would invest in creating links to another's scheme in the expectation that it would be maintained, perhaps by hyperlinking an *Excel* spreadsheet of missions to documents about targets. If the other group later altered the target document format, the spreadsheet references would break. The spreadsheet owner would either have to negotiate with the target group (or if he had the authority, mandate them) to adhere to the format on which he depended, or he would have to repair the references (which would be harder or easier, manual or automated, depending on his technical savvy).

6.2.2.4 Fragmented Memory

Incompatible hierarchies and accumulated clutter made it difficult to navigate the file system labyrinth. Many users dealt with these problems by ignoring the confusion and starting anew. They abandoned previous schemes, created new folders, and started saving the files that they downloaded or received via email, rather than tidying up and consolidating. Files were thus duplicated across the server, many stored with slightly different filenames. After units turned over ("relief in place/transfer of authority" or RIP/TOA), one could find folders literally named "old shit" or "X's stuff" throughout the share drive. The new arrival swept the data of his predecessor under the rug, finding it easier to jump into the flow of new data and start again rather than trying to figure out what was already there. There were instances of archive folders nested several levels deep after several turnovers, containing some of the exact same files which had been rediscovered and resaved by different personnel during each unit rotation. Faced with making sense of a predecessor's hierarchy and clutter, many users opted to reactively construct their own hierarchy and clutter as issues arose. The server filled with data no one used, but which no one wanted to delete out of concern that it might prove useful to someone or to themselves later on. While difficult to quantify, a very large percentage of the data on the share drive was dormant, duplicate, or otherwise of limited value.

The implications for organizational memory can be likened to computer memory. The data for a particular file is usually physically fragmented across a hard drive. The file system maintains an index or pointer to all those physical clusters so that applications can reference the file as a coherent logical whole. When a user deletes a file from the file system, typically the file system only deletes the pointer and marks the data location as empty. The data still physically exists on the hard drive until it is overwritten. This makes computer forensics possible, as deleted files are not ever truly deleted, and they might be reconstructed by analyzing the data clusters on the disk. There was something similar going on with the way people used the share drive. While files might indeed be saved there, the "pointers" to the active files resided with the people who use them. When those people transferred (or become casualties), the address of that data was lost. Other users technically had access to all the residual data on the shared drive, but they were put in the position of forensic analysts, unsure of the meaning or context of fragmented clusters. They might recycle some of it, or they might just sweep it all into an

"archive" folder. Either way, just because "it's on the share drive" does not mean that it is effectively remembered by and available to the organization.[11]

6.2.3 Electronic Mail

Email, using the Microsoft *Outlook* application, was the most used application at the SOTF. Most staff officers received many hundreds of emails each day. Given that many of these included attached files, the email accumulated at a rate of multiple gigabytes per week per person. Personnel dedicated countless hours per day to reading, managing, and responding to email, and it was usually the active application seen whenever one walked by and glanced over (or else it was *PowerPoint*). Microsoft *Outlook* was left running constantly on computers.

6.2.3.1 Informal/Formal Ambiguity

Email combines private asynchrony, allowing writers to take time crafting messages and responses which could be kept on record, with public instantaneity supporting a speedy interchange with a group. These two properties fostered ambivalence in people's approach to email. On the one hand people often adopted a casual manner of interaction, in the form of joking bonhomie or curt sentence fragments, and they persisted in writing colorful or gossipy emails among friends as if the emails were a private conversation. On the other hand, personnel also took email very seriously, as communications of record with directive authority. Thus an officer would spend a lot of time carefully crafting an email, asking others to look it over before it was sent on. Sometimes email exchanges could become very heated over a controversial topic, as when a line officer thought a staff officer was interfering with his sphere of authority. There was often an air of grandstanding formality when these spats were conducted with an audience of others on the carbon copy (CC) line, in keeping with the propensity of email everywhere to promote passive-aggressive "flame wars."

The pragmatics of email interaction—what was said to whom, who was added or removed from the carbon copy (CC) line, who might be on the blind carbon copy (BCC) line, how much time elapsed before a reply, what attachments were included—were all things of great concern for staff officers working to promote their organization's (or their own) welfare. Users

[11]Geoffrey C. Bowker, *Memory Practices in the Sciences* (Cambridge, MA: MIT Press, 2006), makes the argument that the design of databases and classification schemes influences how we remember and interact with the past. The argument in this case is that when the design is obscure and the designer is absent, then collective memory is impaired. For a review of scholarship on organizational memory, see: James P. Walsh and Gerardo Rivera Ungson, "Organizational Memory," *The Academy of Management Review* vol. 16, no. 1 (1991): 57-91.

tended to scan by the sender and subject line before opening emails, those from superiors receiving the quickest attention. Reading and crafting an email was not just a matter of interpreting substantive information conveyed, but very much of attending to the political context and consequences of that communication. Similar to findings with corporate managers, email was often the preferred mode of staff communication even for complex and emotional issues.[12]

6.2.3.2 For Your Information

The majority of emails were addressed to a large subscription list of recipients. These included regular recurring products like intelligence reports and operations summaries, as well as frequent communications to subordinates or communities with similar interests. Membership on a distribution list was not automatic but required knowing about the existence of the list, appreciating its importance, and knowing the list manager. Membership on an email list became something of an in-group marker for who was in the know.

People forwarded a lot of email. One might have to scroll down several pages through lengthy headers and detailed signature blocks to get to the relevant information.[13] The entire email chain also contained information about who was also receiving the forwarding, including which individuals had been added (or subtracted) to the distribution at each step along the way. The ease of forwarding made for a frenetic information-push environment. This is a modern-day manifestation of a phenomenon observed by a British staff officer some ninety years before: "The chief trouble at GHQ was that there was no one there who had time to listen to any new idea. Everybody was busy writing 'Passed to you', 'Noted and returned', or 'For your information', etc, etc, on piles and piles of 'jackets' that no one had a moment to consider any proposal for altering the existing condition of affairs."[14]

---

[12]Lynne M. Markus, "Electronic Mail As the Medium of Managerial Choice," *Organization Science* vol. 5, no. 4 (1994): 502-527

[13] Signature blocks usually included a patriotic/belligerent quote by the likes of General George S. Patton or William T. Sherman, as if to certify the warlike character of the desk-bound emailer

[14] Brigadier-General C. D. Baker-Carr, quoted in Dan Todman, "The Grand Lamasery Revisited: General Headquarters on the Western Front, 1914-1918," in Gary Sheffield and Dan Todman, Eds., *Command and Control on the Western Front: The British Army's Experience 1914-18* (London: Spellmount Publishers, 2004), 39-70, p. 49

6.2.3.3 Personal Data Warrens

Users varied widely in their approach to email management, from leaving everything in the inbox (where it might be easier to find by person or date) to investing time constantly cleaning the inbox and sorting email into folders. Either way, email files became yet another place within the share drive where ever more data might be deposited or abandoned. Moreover, for many people email was the primary information search and storage system. Even if a file might be publically available on the share drive, they would still ask colleagues to email the file to them. One advantage to this would be that the attached file would often come with context not available in the file itself, such as comments in the body of the email about the attachment, information about whom else might be looking at the document, and confidence that one was looking at the right version. This practice, of course, also increased the number of duplicate copies of data strewn across the server. And as *Outlook* mail files were accessible only to the owner of the mailbox, it created more inaccessible warrens of data.

6.2.4 Military Power...Point

After email, Microsoft *PowerPoint* was the most widely used application. The two were complementary, as *PowerPoint* decks proliferated through email. Critics like Edward Tufte revile the widespread use of this tool in corporate and government bureaucracies, arguing that it degrades the quality of analytic thought by reducing arguments to lists of incomplete sentences and stupefying audiences with extraneous and distracting information.[15] Anyone who has sat through a military "death by *PowerPoint*" session will appreciate these concerns.

---

[15]Edward R. Tufte, *The Cognitive Style of Power Point* (Cheshire, Connecticut: Graphics Press, 2003). Tufte's criticism of *PowerPoint* is that common presentation practices diverge from the design principles in Edward R. Tufte, *The Visual Display of Quantitative Information* (Cheshire, Connecticut: Graphics Press, 1992). The range of criticism is reviewed by David K. Farkas, "Toward a Better Understanding of Powerpoint Deck Design," *Information Design Journal + Document Design* vol. 14, no. 2 (2006): 162–171. For miltiary-specific criticism, see: T.X. Hammes, "Dumb-Dumb Bullets: As a Decision-Making Aid, Powerpoint is a Poor Tool," *Armed Forces Journal* (July 2009); Greg Jaffe, "What's Your Point Lieutenant, Please? Just Cut to the Pie Charts," *Wall Street Journal* (26 April 2000): 1; E. Tyler Wooldridge III, "Order a Powerpoint Stand-Down," *U.S. Naval Institute Proceedings* (December 2004); Lawrence Sellin, "Outside View: PowerPoints 'R' Us," *United Press International* (24 August 2010)

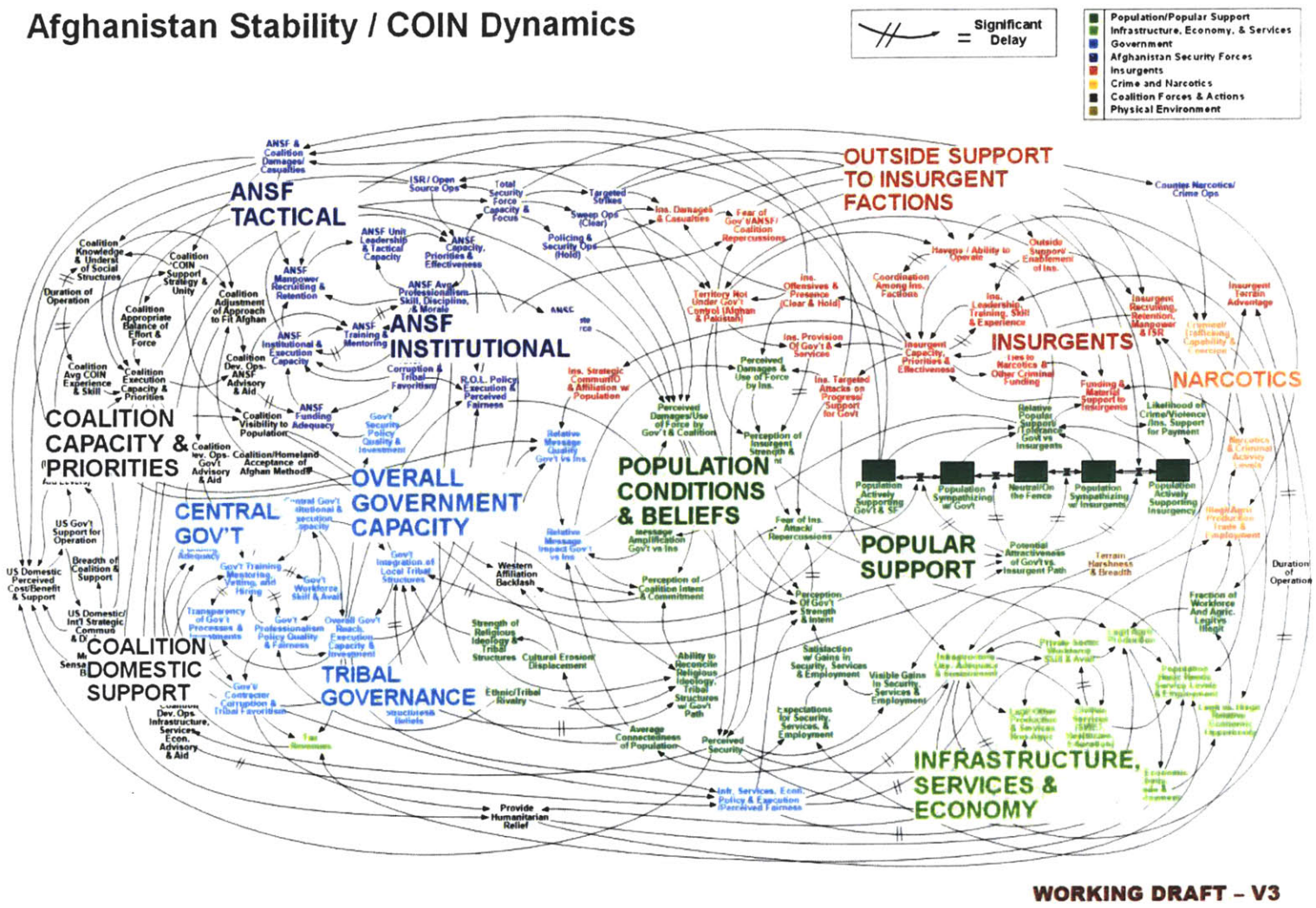


Figure 6-1: A bewildering diagram of counterinsurgency dynamics in Afghanistan

The *New York Times* printed Figure 6-1 on the front page with an article on military reliance on the application, noting that "it ties up junior officers—referred to as PowerPoint Rangers—in the daily preparation of slides, be it for a Joint Staff meeting in Washington or for a platoon leader's pre-mission combat briefing in a remote pocket of Afghanistan." Brigadier General H. R. McMaster said that "It's dangerous because it can create the illusion of understanding and the illusion of control," while General James N. Mattis was more blunt: "PowerPoint makes us stupid."[16] Making, delivering, and taking *PowerPoint* briefs takes up a tremendous amount of staff energy, and is the predominant mode of battlefield experience for many. Strategic plans and patrol reports alike are constructed in *PowerPoint*, and criticism of cartoonish slides has already become *de rigueur* in the historiography of recent conflicts.[17]

While ridiculing *PowerPoint* use may be cathartic, intellectual laziness only goes so far to explain the pervasiveness and persistence of the tool throughout the enterprise. Once the social context of *PowerPoint* usage is taken into account, military reliance on its versatility is more understandable. It is not the tool per se that makes people stupid, but its embedding in layers of complex representation which remove personnel from the battlefield. Personnel embrace *PowerPoint* to deal with emergent representational and communicative challenges, but an unintended consequence is enhanced risk of insulation. As always, technology both enables and constrains.

6.2.4.1 A General Purpose Graphical Editor

PowerPoint should be appreciated as a general-purpose graphical editing tool that was universally available to and understood by military computer users. It enjoyed strong network effects, meaning that the value of the tool to any one individual was enhanced by the number of other people using it. The ubiquitous installation of the Microsoft *Office* suite assured wide compatibility and communicability of *PowerPoint* files, while by the same token crowding out other tools that provided more power and functionality for particular applications. For instance, while *PowerPoint* could be and often was used to store and share a database of intelligence

---

[16] Elisabeth Bumiller, "We Have Met the Enemy and He is PowerPoint," *New York Times* (26 April 2010), A1. "When we understand that slide, we'll have won the war," General Stanley A. McChrystal, the commander of American and NATO forces in Afghanistan in early 2010, said wryly. Note the consultant's logo on the bottom left, and thus the blending of corporate and military staff cultures.

[17] For example, Michael R. Gordon and Bernard E. Trainor, *Cobra II: The Inside Story of the Invasion and Occupation of Iraq* (New York: Random House, 2006), 556-564, reproduce a number of slides typical (and typically vague) of contemporary operational planning.

information, doing so sacrificed the powerful analytical, quality-control, and search capabilities of a dedicated database package. To update an old adage, if all you have is *PowerPoint*, then every representational problem looks like a slide presentation.

Indeed, the ways in which *PowerPoint* was used beyond its designed purpose as a presentation aid was remarkable: for operational coordination graphics, tactical mission aids, photo editing, intelligence databases, operations summaries, and more. *PowerPoint* has been reshaping many different military genres besides just briefing or presentation (where it still is well employed).[18] Its ubiquity, both in terms of availability and user competence, enables new representational practices, while at the same time constraining them, as critics rightly worry. As troubling as the prospect may seem, *PowerPoint* has in fact become a general-purpose military command and control system.

6.2.4.2 An Ersatz Database

Many *PowerPoint* files were recurring templated products. These often involved a graphic (usually a map or satellite image) annotated to indicate salient features or events, perhaps inset with photos of individuals, places, or equipment, and with a text box packed with data fields on one side of the slide. For example, a daily or weekly intelligence summary (INTSUM) slide would show a map of the area of operations with callouts to significant activities, shapes depicting enemy concentrations or areas of tribal control, and a chronology of reporting in the text box. A target slide could show a picture of an individual,[19] a chart of his connection to other insurgents, an image marked up with salient terrain and threat features, and text summarizing reporting and assessing the target's significance. A concept of operations (CONOP) would provide a one slide overview and reference document for a planned operation: a map of the target area with the target and distance from the staging area indicated, a text box listing the target description, significance, composition of the assault force, communications details, *etc.* A storyboard slide would provide a summary of a completed mission with an area map, photos of

[18] Joanne Yates and Wanda J. Orlikowski, "The Powerpoint Presentation and Its Corollaries: How Genres Shape Communicative Action in Organizations," in *Communicative Practices in Workplaces and the Professions: Cultural Perspectives on the Regulation of Discourse and Organizations*, ed. Mark Zachry and Charlotte Thralls(Amityville, NY: Baywood Publishing, 2006), discuss an example of this genre-stretching from the corporate world, where *PowerPoint* "decks" of slides are printed off for table-top briefings or leave-behind information, never intended to be publically projected. This same application is found in military contexts. Yates and Orlikowski's findings from corporate bureaucracies generalize well to military organizations, although the use of *PowerPoint* is probably richer in the latter, given the additional military-specific genres in which *PowerPoint* is used.

[19] A mock example is included in the next chapter

detainees and recovered equipment, and a narrative summary of the participants, phases and results of the mission.

With very small fonts and detailed annotation, these products tended to have a very high information density (whether considered in number of words, discrete concepts, or slide elements). This stands in contrast to the rather low information content of bulletized briefing slides, a major point of criticism from the Tufte school. These military-specialized, templated, synoptic data slides were far more structured than a typical briefing slide. At the same time, the choice of small fonts seemed to be designed to accommodate large blocks of text cut-and-paste from other reports, without citation, rather than summarized for the particular product.

Templated slides generated for recurrent events served as an ersatz database of information on those types of events. This was a "database" only in the most rudimentary sense that similar, semi-structured data was collected and saved together; there was no rigorous data definition as in a genuine relational database. At the digital application level, each *PowerPoint* slide is just a collection of shapes with no concept of data type, so it is virtually impossible for a machine to parse the data and perform useful operations across a set of records (such as sorting, summing, comparing, *etc.*). *PowerPoint* data is designed to be viewed and operated on by human beings, one slide at a time. Thus any sort of aggregate questions (*e.g.*, how many missions have we done in this target area? How many targeted individuals have we apprehended?) could only be answered by a human being opening each file/record and making a tally. Another problem was that in creating a new record, a person would usually take a previous slide as a template, risking inadvertently importing data from a previous mission or target and thus corrupting the data. Furthermore, each of the fields or annotations had no data integrity controls (defining type, number, geocoordinates, authorship, modification date, *etc.*) because they were just shapes on a *PowerPoint* slide, so there was little accounting for inadvertent changes or "fat finger" errors. Additional problems emerged across different types of products that shared similar data elements (as when a CONOP and intelligence slide were both about the same target), because when the common elements changed, they had to be manually changed (if at all) in multiple different product lines. Failure to synchronize interdependent products compromises data integrity.

If *PowerPoint* is such an inefficient way to store data, why was it so prevalent? Perhaps it was widespread ignorance about data management, an admittedly specialized domain of methodological and technical knowledge. Most personnel only were concerned with one record at a time to deal with the mission, the deliverable, or the briefing at hand; aggregation or analysis of historical data was someone else's concern if it was one at all. A more important reason was that personnel had to deal with emerging information requirements within a short time horizon. A close look at INTSUM, CONOP, or target slides would reveal that few were ever structured precisely the same. Fields were formatted differently, added or dropped, and idiosyncratic information elements were included on a slide by slide basis. In effect, the database-like elements of each slide were up for redesign with every individual record. These *ad hoc* updates to data format might stem from idiosyncrasies of the particular mission or target, or from new policy guidance to start tracking a new kind of data. The design of the product template was completely unconstrained by *PowerPoint* itself; it was completely a matter of organizational policy, or lacking that, authorial preference. Thus slide authors could readily deviate from the template to deal with deviant cases, or managers could mandate authors to include (or suppress) particular sorts of data. Furthermore, by collecting data directly onto a *PowerPoint* slide, the storage medium was also the display medium, so it could be easily communicated and briefed.

SOTF personnel at large were collectively playing the role of database designer with these *PowerPoint* slides and enacting a slow, noisy database engine. These practices could accommodate emerging information requirements, deviant cases, communication of slides/records between any email recipient with *PowerPoint* installed, the collection and display of complex mixed-media data, *etc.* Yet this came at the cost of compromised referential integrity and inefficient manual review of individual records for aggregative operations. The ability to vary or ignore data structure at the record level eroded the comparability of the each slide/record with another.[20] No database architect in his right mind would choose to implement a database in *PowerPoint* for these reasons. Yet when the database designer was the collective mind of personnel with highly uneven levels of technical skill, coordinating across different locations with only a basic level of software compatibility, and contending with a turbulent information environment, *PowerPoint* turned out to be the tool of choice for real-time database design.

---

[20] Enforcing comparability of elements is needed to gain control over them, Wendy Nelson Espeland and Mitchell L. Stevens, "Commensuration As a Social Process," *Annual Review of Sociology* vol. 24 (1998): 313-343

6.2.4.3 A Word Processor

Microsoft *Word* was, unsurprisingly, used to draft memos, reports, and other documents. More interestingly, many products that might have been better created in *Word* ended up in *PowerPoint* instead, as briefs with a large number of slides with dense text blocks. The decision to ignore the word processor's powerful organizational and text control features (not to mention fluid use of prose in an extended argument) appeared to be grounded both in the greater relative comfort personnel felt with *PowerPoint* as an all-purpose tool and in the anticipation that information might have to be briefed, or cut and paste into other briefs, rather than simply read.

6.2.4.4 Dual-Use Slides

PowerPoint was of course employed in its more familiar briefing genre as well. Military briefs were usually developed for two different kinds of audience. First was the traditional briefing audience, where the slides were a supplementary aid to the presentation (or more often than not, the briefer is more of a supplementary aid to the slide). Second was the audience who would look at the presentation asynchronously, downloading or receiving it via email; the presentation had to stand on its own. The purpose of a briefing was not only to store and display information, but through this to coordinate the behavior of people distributed across different sites. The resulting compromise invariably delivered far too much information and clutter for an engaging presentation, while lacking enough detail and organization to render the standalone product understandable.

PowerPoint critics like Tufte would prefer to see presentations carefully crafted to effectively present information to the audience, forgoing slides altogether whenever possible. Military users would certainly do well to pay more attention to presentational rhetoric; nevertheless, such advice overlooks the ways in which the tool was often used in a time-constrained and collaborative environment. *PowerPoint* briefs were not finished products designed to deliver information one-way to an audience. Instead they were often expedient drafts which facilitated collaboration among people. At the SOTF *PowerPoint* provided a quick way to get a draft of ideas together which would then serve as a framework for group discussion in the conference room. For a quick turnaround on concept development or status update, the working notes and the presentation were one and the same.

Likewise, if graphical and textual information needed to be quickly communicated—a picture taken on a recent operation with some salient detail annotated—it would be easy to do so with *PowerPoint* and email. Often expedient slides sent from Task Units would be folded right into briefs at the SOTF. This was easy to do with *PowerPoint*'s interface concept of a series of slides which can be rearranged, providing a way to quickly mix and match slides from various existing briefs to tailor make a new presentation. The major downside of this practice was that individual slides (or slide elements) lost provenance as they were swapped about.

6.2.4.5 A Forcing Function for Collaboration

The process of drafting a *PowerPoint* could serve as a collaboration aid. On several occasions senior staff members sat around a table with a brief projected on a screen, arguing about the wording and design of the slides and editing them on the fly. While some discussions of color, format, animation, and other "slideology" bordered on the trivial (or they argued about how to compress a perfectly good sentence into an incomprehensible bullet), at the same time this process structured the discussion and helped group members to come to a shared understanding of whatever policy matter occasioned the brief.

These live editing sessions often occurred before a visit from some person of importance to the SOTF. Such visits occasioned calls from the executive officer for each staff section to update their slides in the command brief.[21] This activity reinforced a collective expectation that "distinguished visitors" (DVs) would sit for a *PowerPoint* briefing and more importantly, that the *PowerPoint* session would provide the most important information to the visitor. While command briefs tended to paint a rosy picture of the unit's activities, often accepted uncritically, they also served a function of gathering key staff members together face-to-face with one another and with key representatives to facilitate mutual understanding.

6.2.4.6 Provenance Loss

The military is a practical organization and the government owns all the information it generates. These factors inadvertently foster a culture of plagiarism. Thus, it was the rare brief that was ever wholly original. Most of the slides included from elsewhere would inevitably be stripped of their authorial and temporal context. For intelligence briefings in particular, it could

[21] A standard military genre providing an overview of a unit's mission, environment, organization, and activities with several slides from each staff section.

be impossible to discern the origin of bulletized judgments, as too often authors just downloaded other organizations' *PowerPoint* intelligence summaries and reformatted them to look like their own. Cutting-and-pasting slides across briefs could also inadvertently reclassify slides because of the widespread use of "master" templates to automatically include a text box marking classification on every slide. A quirk of *PowerPoint* is that slides copied from one presentation to another will use the master template of the destination file rather than the source, thus instantly reclassifying every slide in the presentation. A further related danger would be that slides that emerged as temporary expedients to communicate information or facilitate discussion would be incorporated into more finished briefs without revision or inquiry into their continuing validity. Old slides never die, they just get reformatted.

Another sort of provenance-loss occurred when authors cut-and-paste graphical screen shots from other applications into *PowerPoint* for a single use. For example, the *FalconView* geospatial information system would be used to mark up a map with a complex overlay describing geographic points and events of interest. Users would then insert a static screenshot of this *FalconView* map data onto a *PowerPoint* slide. The recipient of the slide would get the snapshot of a particular space and time but would not have access to other geospatial metadata in the *FalconView* overlay outside of the snapshot boundaries, nor would he be able to manipulate or update the overlay or view it at a different scale. The usefulness of the static snapshot was limited to the data it displayed, and the origin and any metadata associated with that data was inevitably cut asunder in the process. These snapshots also inflated file sizes by passing not just the novel overlay information but also a copy of the baseline map data which everyone already had on their own systems, consuming valuable bandwidth with redundant data.

6.2.4.7 PowerPoint Rangers

PowerPoint is ubiquitous in contemporary military environments. It served some functional roles in coordinating collaboration across a widely distributed organization facing a turbulent environment. The database-like functions of the military-specific *PowerPoint* applications especially exemplify this role. This larger social context of *PowerPoint* is often overlooked in criticizing the application's deleterious effects on analytical thought.

Nevertheless, it is hard not to become uncomfortable with the dominance of *PowerPoint* in American military culture and command and control, per its critics. Staff officers were

unlikely to write a paper making a clear argument for an initiative or operation, settling instead for ambiguous bullet points and rough diagrams. Ambiguous bullets could excuse a staff officer from committing to specific causal statements or policy positions, allowing it to be tailored to any briefing audience. A great deal of effort was invested in reformatting existing slides or engineering vacuous cartoons, which could play a dazzling rhetorical role but add very little value in terms of content and analysis. "The brief" itself could become the end product rather than the ideas or concepts it was supposed to convey. Building the brief was an occasion for great bureaucratic self-flagellation, and sometimes more insidiously, a flashy diversion from hard questions about blood and treasure. It is little exaggeration to say that competence at *PowerPoint* "slideology" has become a required core competency for American staff officers. The elaborate design and density of shapes and text on military staff slides furthermore seems to increase as they originate at higher echelons of command, and one can only wonder at the countless staff officer hours invested in rearranging and resizing shapes on a slide. A tempest of decorative formatting and provenance-destroying plagiarism consumes great effort but bears only the most tenuous connection to operational reality.

When "knowledge is only *PowerPoint* deep" there is real danger of developing false confidence and misunderstandings about the war fighting problem one is facing. As one soldier observed about his experience, "I went there with the wrong attitude and I thought I understood Iraq and the history because I had seen *PowerPoint* slides, but I really didn't."[22]

[22]Thomas E. Ricks, "Flaws Cited in Effort to Train Iraqi Forces," *Washington Post* (21 November 2006): 1

6.2.5 Layers of Maps

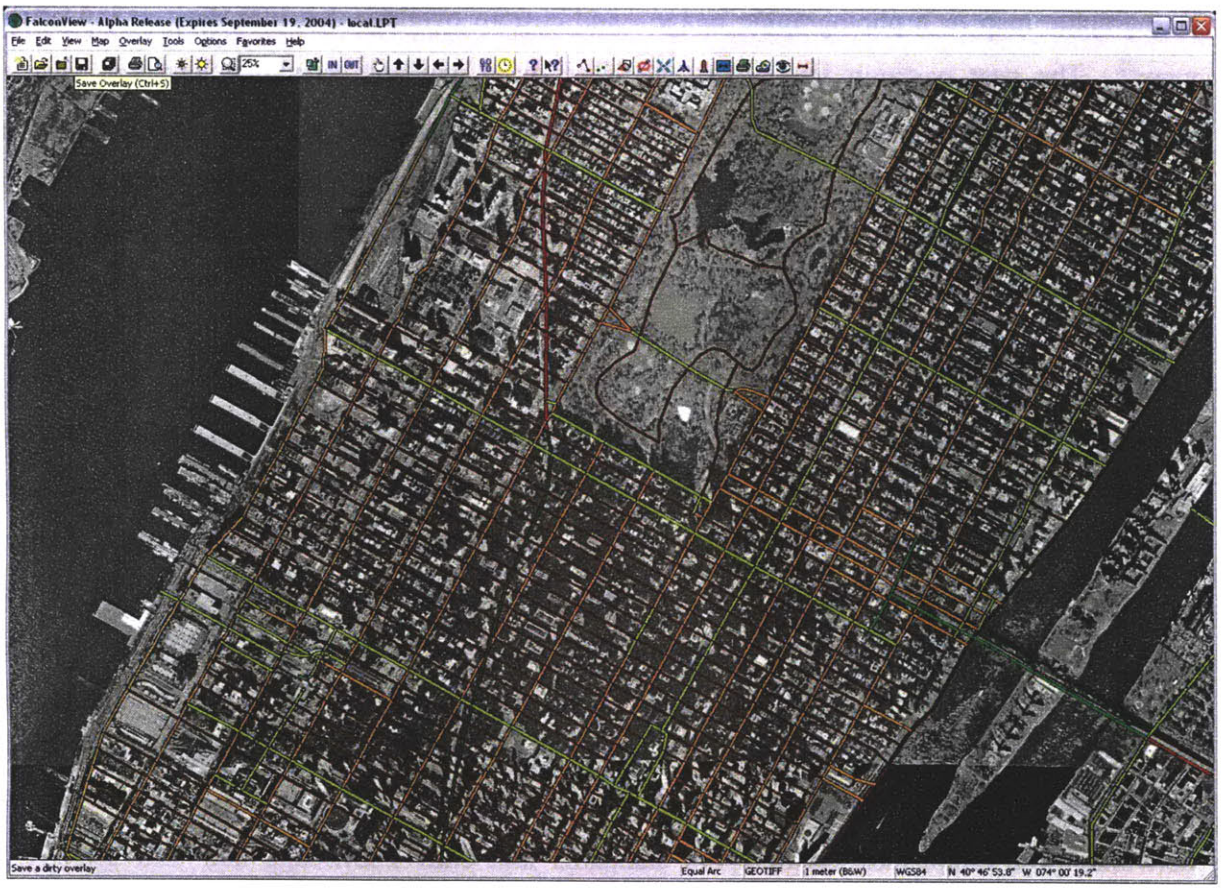


Figure 6-2: *FalconView* screenshot showing a satellite image and a street overlay[23]

For an enterprise focused on controlling ground, maps are one of the oldest and most important types of military representation.[24] Paper maps hung on nearly every SOTF office wall, digital maps were included in any tool where feasible, and a large proportion of *PowerPoint* files included screenshots from geographic information systems (GIS) like *FalconView*, Google *Earth*, or *ArcGIS*. GIS separate map data into layers of information that are bound together in a

[23]Georgia Institute of Technology, "Not for Pilots Only: Flight-mapping Software Attracts Broad Audience with its Diverse Capabilities," *Georgia Tech Research News* (20 June 2004), http://gtresearchnews.gatech.edu/newsrelease/falconview.htm [accessed 8 December 2009].

[24]Jeremy Black, "A Revolution in Military Cartography? Europe 1650-1815," *Journal of Military History* vol. 73, no. 1 (2009): 49-68; Michael Biggs, "Putting the State on the Map: Cartography, Territory, and European State Formation," *Comparative Studies in Society and History* vol. 41, no. 2 (1999): 374-405; Daniel R. Headrick, *When Information Came of Age: Technologies of Knowledge in the Age of Reason and Revolution, 1700-1850* (New York, NY: Oxford University Press, 2002); John Noble Wilford, *The Mapmakers, Rev. Ed.* (New York, NY: Vintage Books, 2000); John Brian Harley, *The New Nature of Maps: Essays in the History of Cartography* (Baltimore, MD: Johns Hopkins University Press, 2001)

common coordinate grid. The basic distinction is between a base layer—which can be a cartographic map or a photographic image—and custom overlays that plot data on top of the map.[25] The neat partition into layers mediated by a standard coordinate protocol enables cartographic institutions to pre-process broadly useful representations without having any local knowledge. Users can then construct overlays to display unit specific annotations, points of interest, battlefield control measures, schemes of maneuver, and ephemeral intelligence sensor data over any scale of map or image (Figure 6-2).

6.2.5.1 Reliable Base Layers

It's often said that "the map is not the territory," yet base layers were relatively good guides to the topography of Iraq.[26] While terrain did change between map revisions—a large lake indicated on charts of Anbar Province was in fact only a tricking stream—such changes could be detected with overhead imagery and incorporated into common representations (although these updates sometimes remained informal matters of what "everybody knows" rather than formal updates). The National Geospatial Intelligence Agency (NGA) produced detailed map and satellite image data which was widely available in standard formats readable on common GIS. The substantial infrastructure of satellites, mapping agencies, communication networks, well-established cartographic standards and craft knowledge and GIS effectively bound changes in the terrain to changes in the map, so that personnel could almost take it for granted that their base layer map would support inferences back to and behavior with real topography without great surprise.

6.2.5.2 Idiosyncratic Overlays

Locally-produced overlays had inherent potential for mutual interference, however. Personnel had to deal with the residual mismatch between map and terrain and the ease or

---

[25] GIS is a digital version of the classic map board with acetate overlays marked up with grease pencils. Most GIS represent coordinates as decimal latitude and longitude degrees (*i.e.*, -36.56, 109.94), so anything that can be expressed in that format can be plotted. This leads to lots of formulas in custom *Excel* spreadsheets that translate coordinate formats from human-readable formats (like 34°45'21" N, 103°32'12" E) in order to plot them, an instance of users acting as interoperability daemons. Datum, which identifies the mathematical ellipsoid model approximating the irregularly shaped planet, is a also critical piece of information—the same coordinates on different datums can plot miles apart on the surface of the earth—but the WGS-84 datum is nearly universally standardized and was generally assumed without problem.

[26] Anbar is flat with the population mainly distributed in urban centers along the Euphrates. Terrain is more extreme in Afghanistan, where tactically-relevant variation often exists below the resolution of topographic maps and roads on a map often turn out to be muddy single-track trails.

difficulty of communicating particular updates. The disaggregation of digital layers into separate files enabled almost anyone to create them at their workstation and send out copies, or to lose them in the share drive. The simple GIS abstraction of a single coordinate grid with layers was agnostic regarding the way it was used. Thus users had to make design decisions about the symbols and colors they used, the precision of the coordinates, the amount of identifying metadata, *etc.* Communities that regularly used a given overlay could harmonize interpretations, but metadata would inevitably be left out when the overlay was moved out of context. Overlays downloaded from a website, received via email, or discovered on the share drive often had little provenance metadata to clarify their references (Table 6-1). User overlays provided flexibility but for the same reason also abetted divergence of common maps into pools of local relevance.

Table 6-1: Potential confusion about map overlays missing provenance metadata

Examples of questions about overlays taken out of context
• Which battlefield control graphics are current and when were these made? Do we still use these house numbers and route annotations?
• Why does this overlay of provincial boundaries include all these battlespace boundary markings I don't care about?
• What was the source data for all these plotted locations of an individual here?
• Are these SIGINT, MASINT, or HUMINT reported positions?
• Did a human analyst build this overlay (which means I can assume it's been cleaned up but is probably incomplete), or was it populated by some automated batch query (which means it's a complete and cluttered dump from a database)?
• What kind of events are all these crazy icons being used for?
• Are these the actual, precise locations of these events, or just the center of the neighborhood or city where they happened?
• Are these sharply demarcated tribal boundaries really so well defined in the minds of locals?

6.2.5.3 Pasting into PowerPoint

Technical GIS interfaces also generated friction. *ArcGIS*, *FalconView*, and Google *Earth* all had their own overlay formats, each required application-specific technical skills, and they weren't all universally available. Invariably it was *PowerPoint* to the rescue. Users often just pasted GIS screenshots into *PowerPoint* slides rather than sending overlays. By doing so they

focused viewer attention on the particular overlay symbols and the map scale the GIS user wanted to display and also ensured that the receiver would be able to view the map data. But the screenshot also froze all the data into a single snapshot, discarding provenance and geo-reference data as well as any annotations outside of the screenshot area. The screenshot also bloated file sizes (*i.e.*, as large raster images *vs.* compact vector files). To further locally-tailor the snapshot, many users made annotations within *PowerPoint* drawing tools. The slide then provided the visual appearance of a GIS overlay but without any of the metadata or geo-referenced anchors. There could be neither further analysis of the geographical context with GIS, nor any certainty over the accuracy of the annotations.

When overlays were viewed atop a base layer—especially when the two were merged in a *PowerPoint* image—a careless viewer could be lured into thinking that the overlays were as well-produced as the base layer. The overlay borrowed rhetorical credibility from the base layer, but the fused representation hid questionable design decisions that went into it. Maps are essential military tools. They have a lot of predictive and coordinating power because of the stabilizing work of institutional infrastructure and common coordinate standards which bind together maps, sensor data, and overlays with real-world topography that does not change rapidly. The detail and fidelity of the general base layers could not be matched by the particular overlays, however. No representation mapped perfectly onto "ground truth," as they were all constructed for particular and not always commensurable purposes. Technical and epistemic obstacles to integration caused personnel to spend time reformatting, chasing updated versions, or simply rebuilding overlays.

6.2.6 Secret Internets

SIPRNET and JWICS are on one hand like classified versions of the public internet where military units and various agencies run their own websites and services in a decentralized fashion, and on the other like vast corporate intranets centrally managed by the Department of Defense, enforcing security and configuration policy. Organizational websites are accessed through browsers, as on the public internet (with addresses that end in "smil.mil" or "sgov.gov" for the SIPRNET or "ic.gov" for JWICS), yet differences arise because website hosts and users are employees of (or contractors for) a vast security bureaucracy.

6.2.6.1 Sluggish Search

Search engines appeared to work far less efficiently on the SIPRNET. On the public internet a savvy user can usually find relevant content within the first page of search results, making sites like Google and Yahoo basic starting points for accessing the internet. The same search engines were available on the SIPRNET (albeit years after their public introduction), yet results typically took longer and returned a large amount of irrelevant results.[27] Users tended not to use unrestricted search engines but instead tended to manually browse to specific websites to check for updates or to search particular reporting databases the contents of which were typically not indexed by the generic search engines. One could find diplomatic cables on a State Department site or satellite images on a National Geospatial Intelligence Agency (NGA) site if one knew where to look and how to search.[28] Of course much information was hidden behind password and certificate-protected firewalls, and it could be difficult to find the right bureaucratic keys to unlock them. Finding the right information usually depended on the local knowledge of SOTF users who knew where and how to search; lacking this, information posted on the SIPRNET could be effectively lost.

6.2.6.2 Tentative Embrace of Web 2.0

SIPRNET has been slow in adopting so-called "Web 2.0" capabilities—blogs, wikis, social-networking sites, video-sharing, and programmable interfaces—which have received a lot of attention on the public internet in the past decade. These collaborative technologies feature intensive interaction with user communities to determine online content, in contrast with 1990s-era sites where user interaction was more limited to browsing and downloading hosted content. In general government website sophistication tends to lag developments on the public internet by years, as civilian software must go through a regime of testing and certification before migrating over to military networks. Web 2.0 lowers the barriers to entry for authoring content, which may

---

[27] Why should the same search engines which work so well on the public internet behave so inefficiently on SIPRNET? Determining the reason for poor search results would take more technical investigation than I could do at the SOTF in my official capacity. It may be simple technical inefficiency, but it may also be different patterns of hyperlinking on the SIPRNET. For instance, as one officer speculated, many search engines rate the importance of pages through "back links," which are the number of links to a page from other pages, but the pattern of links may be different on an internet focused on simply posting finished products rather than robustly linking to other existing pages (that is, where there is no culture of including hyperlinks to other products as on public internet blogs). Of course, many products of interest were also hidden within password-protected servers that search engines couldn't effectively index.

[28] A public analogue would be bypassing Google to perform searches directly on the New York Times website or JSTOR.

also undermine bureaucratic control of content. Some older government employees furthermore seem unfamiliar or uncomfortable with emerging IT.

Red-tape and generational delays alone do not account for the tentative use of collaborative web technologies, however. Users face fundamentally different incentives on the SIPRNET. Would-be SIPRNET bloggers, for instance, cannot adopt anonymous pennames and are highly unlikely to post controversial, opinionated, or humorous content that might prove embarrassing to themselves or their organizations. The social, entertainment, and reputational incentives that internet bloggers respond to are diminished in the more formal SIPRNET environment.[29]

6.2.6.3 Wikipedia Transplanted

The difference between public Web 2.0 and the SIPRNET—and thus the role of social context in shaping technical capabilities—was most stark between *Wikipedia* and *Intellipedia.* Wikipedia is an open-source encyclopedia anyone can edit, and its accuracy has been found to be comparable to edited encyclopedias on non-controversial topics.[30] Intellipedia attempts to reproduce Wikipedia on the SIPRNET using the same MediaWiki software that allows any user to add or edit any content. Intellipedia boosters envision a forum providing the latest intelligence on any topic and robust exchanges among analysts, overcoming the delays and red-tape associated with agency-branded intelligence production routines.[31] However, Intellipedia users face quite different incentives on whether to contribute and what sort of information to contribute. Rather than a reliable public good of "crowd sourced" intelligence, users embraced Intellipedia more as a free website hosting service to work around network administrators to post their privately-branded products.

---

[29] There has been a surge in internet blogging by military personnel (milblogs) during the wars in Iraq and Afghanistan. Uncomfortable with the unfiltered, instantaneous, and potentially compromising comments of junior troops on the public internet, most organizations have placed restrictions on blogging and access to social networking sites, driving some milbloggers underground. I personally saw little of this activity given the more insular and security-conscious culture of special operations. James Dao, "Pentagon Keeps Wary Watch As Troops Blog," *New York Times* (9 September 2006): A1; Matthew Currier Burden, *The Blog of War: Front-Line Dispatches from Soldiers in Iraq and Afghanistan* (New York, NY: Simon and Schuster, 2006)

[30] Don Tapscott and Anthony D. Williams, *Wikinomics: How Mass Collaboration Changes Everything* (New York, NY: Penguin Books, 2006); Jim Giles, "Internet Encyclopaedias Go Head to Head," *Nature* vol. 438 (2005): 900-901; Fernanda B. Viegas, Martin Wattenberg, Jesse Kriss and Frank Van Ham, "Talk Before You Type: Coordination in Wikipedia," Hawaii International Conference on System Sciences (2007)

[31] Clive Thompson, "Open-Source Spying," *New York Times Magazine* (3 December 2006)

Wikipedia's open-source market for public knowledge goods runs into problems in a bureaucratic environment where users depend on specialized, secret, time-sensitive data. Wikipedia content is managed through a form of peer review whereby volunteer "gardeners" discuss and enforce norms to ensure that contributions are public, objective, non-opinionated, and verifiable. These same criteria would exclude most interesting intelligence.[32] On the supply side, Wikipedia's authors and editors are willing to contribute to a public good because, similar to any open source project, they benefit personally by having topics of interest to themselves represented online and through participating socially in a community of "Wikipedians."[33] These benefits outweigh the costs of acquiring the rudimentary technical knowledge needed to mark up any wiki page and of understanding and conforming with editing norms. By contrast, overcoming these barriers is often not worthwhile for SIPRNET users who were too busy or not technically inclined. As long as analysts were on the hook to file reports and provide briefings to their customers, Intellipedia contribution became simply an additional burden for which they and their organization were not compensated or recognized. Additional barriers came with classified and deployed networks; for instance, Intellipedia editing access was intermittent on SOTF SIPRNET nodes for unresolved technical reasons, undermining confidence that Intellipedia would be available and up to date. Many potential contributors with unique and important knowledge simply ignored Intellipedia (opting instead to use email, and *PowerPoint*, which were perceived as more reliable, a self-fulfilling prophesy given increased attention from technical staffs to maintaining email accessibility).

On the demand side, Wikipedia's vast population of non-contributing users benefit by having access to common knowledge on public topic with a reasonable first-order level of

---

[32] Intelligence bureaucracies exist because some of the information that operational and policy customers need is not readily available through open markets. There are tremendous transaction costs in intelligence production: the expense and risk of secret collection, the coordination of different information sources and analytical perspectives, the emergent and ambiguous nature of intelligence targets, and the niche needs of operational customers operating under strong time and accuracy constraints. These same factors make intelligence something of a private good: secret sources are not available to all, analytic judgments are the products of specific intelligence shops responsible for specific requirements, opinions about fleeting topics can be controversial, and intelligence is produced for (and often only relevant to) a specific operational/policy customer. Contrast this to the information on Wikipedia: facts can be verified with open sources, common knowledge is not branded or owned by anyone, and encyclopedic topics are of enduring general interest.

[33] On individual incentives to participate in open source projects: Eric Von Hippel, *Democratizing Innovation* (Cambridge, MA: MIT Press, 2005); Josh Lerner and Jean Tirole, "Some Simple Economics of Open Source," *The Journal of Industrial Economics* vol. 50, no. 2 (2002): 197-234

accuracy. They can free ride without diminishing the public good, and if someone else doesn't contribute information on a particular, they are no worse off than they were without Wikipedia. For Intellipedia by contrast, if users chose not contribute their specialized knowledge, it simply would not be included because few others would be working in their specific, bureaucratically-assigned niche. Those who did choose to contribute would have to redirect their effort away from traditional products and quality control mechanisms that their customers were depending on. Customers who lacked confidence in or access to Intellipedia were unlikely to endorse any effort to reorient intelligence production, which would require the socialization of new managerial norms to deal with perishable, mission-critical, secret, and private information. Wikipedia supports free-riders in a way that Intellipedia does not.

Although Intellipedia didn't work like Wikipedia, this doesn't mean that it was ignored. Instead, many SIPRNET users embraced it as a free website hosting service. On the SIPRNET high coordination costs were associated with hosting and maintaining a traditional website with a registered .smil.mil domain name because this required approval and cooperation from an IT bureaucracy; Intellink empowered users to bypass their IT departments to post their own website materials. Whereas Wikipedia pages tend to have "objective" textual content about people, places, events, and other things in the world, Intellipedia pages by contrast include a lot of "subjective" unit-specific portals of administrative material and links to downloadable *PowerPoint* files, creating an aura of private ownership for each page. Users were thus less inclined to edit other users' pages, but instead started their own new pages on similar topics, maintaining them only for as long as the original author maintained an interest and then leaving it dormant. Such Intellipedia enclaves might receive a lot of use by small groups using them to coordinate their specific activity, but this was a far cry from provisioning public encyclopedic knowledge. This was yet a further manifestation of the more private nature of information produced to support specific operational customers, rather than the public nature of Wikipedia topics. The vaunted self-organization of Wikipedia was notably lacking in Intellipedia, which instead became another warren of private information stores cluttering up a public space.

6.2.6.4 Foggy Portals

Intellipedia "portals" were just one instance of this "one-stop shopping" type of web application for posting an organization's files and announcements. Web "portals" provided

something like a web-accessible share drive, with folders and files that had to be uploaded individually. While portals provided wider access across distributed locations, navigating it and downloading or uploading files through a web interface could be time consuming. Thus each organization continued to maintain elaborate share drive files and to communicate the same files via email, creating yet another opportunity for divergence between ostensibly authoritative data stores. Like the share drive, portals had a tendency to accumulate duplicate files and private warrens.

"Knowledge management" advocates in the NSW and broader SOCOM communities advocated for portal usage.[34] In pursuit of an ideal of total information sharing, SOTF and Task Unit staffs were directed to maintain files on a portal called the WIC (Warfighter Information Center). The SOTF's higher headquarters (CJSOTF) also advocated portal usage. Unfortunately there were two completely different sites and formats preferred by the two different Army Special Forces (SF) Groups which rotated through as CJSOTF. Thus each portal would go dormant for seven months at a time, although both would remain active on the SIPRNET as official CJSOTF sites. Not only would one site lag behind with the latest information, but also the guidance and plans on the two sites could differ a lot because the two SF Groups had different approaches to operations in Iraq (one emphasizing kinetic kill/capture and the other a more indirect "by, with, and through" approach). This led to frequent confusion as SOTF personnel with an occasional need to access CJSOTF data spent time clicking through folders on the wrong site. Ongoing exhortation on the part the executive and operations officers was required to keep portals up to date in the name of collaboration and knowledge management. Staffs nevertheless continued to depend on email work-arounds to accomplish the same purpose. Portals were often advertised by their boosters as "one stop shopping" for command data, but they invariably provided only a fragmentary and clumsy portion of it, and they could easily fall behind the pace of operations. Portals did provide enough information, however, for the SOTF's administrative command back in California to keep tabs on operations, levying yet more queries for additional information onto an already overburdened staff. Technology-centered "knowledge management" efforts invariably ended up pushing the burden of actually managing information right back onto the organization.

---

[34] The term "knowledge management" in military discourse has come to refer mainly to website management rather than to the hybrid human-machine information processing throughout the enterprise.

SIPRNET websites (usually in the "Web 1.0" mode of publishing organizational content for download) did indeed provide a great deal of valuable information. As with the public internet, the sheer volume of information could be overwhelming, and the evaluation of information sources was complicated by frequent cut-and-pasting, but if one knew where to look, there was no shortage of current and background intelligence, policy, and operational information available. A forward deployed analyst could now have access to almost all of the same sources of intelligence as analysts located back in Washington D.C. Nevertheless, the volume of information and the difficulties of search encouraged many staff members to simply respond to information pushed to them via email rather than searching it out on the SIPRNET themselves.

6.2.7 A Profusion of Applications

While the SOTF's most prevalent data-management tools were paper, the share drive, email, *PowerPoint*, and web applications, other tools deserve some comment. Each generated some familiar interference patterns, and also highlighted idiosyncratic issues.

6.2.7.1 Data Stored in Visual Layouts

The *Excel* spreadsheet was a key tool in the staff officer's quiver. Spreadsheets were often impressively complicated with hundreds of columns and multiple sections. Some of the most important products in operations departments were spreadsheets which coordinated the movement of people and equipment, such as "synch matrices" (*i.e.*, Gantt charts showing rows of different activities across columns of time units) and flight manifests (assigning personnel to airflow). An important aspect of these spreadsheets for data management was that they often exploited the visual layout of data elements (i.e., grouping, sizing, placement, or coloring of different types of data, and inclusion of non-meaningful data like empty cells to structure the layout) to convey information. For example, a logistics officer planning the movement of groups of people in an out of the theater might create a spreadsheet with columns representing days and rows representing the different groups. Several cells across one row could be merged and then colored to represent a certain type of transportation for that leg of the journey. The entire matrix would fill up with different colored blocks that showed different groups transferring across different transportation platforms and command custody along the way. The visual display would also display what aircraft might or might not be available to move other groups around.

Such layout data was designed to be useful to people, not machines. To incorporate it into a database or statistical package required a great deal of manual pre-processing because the visual data was basically invisible to machine processing against simple rows and columns. If the spreadsheet was a recurrent product (probably received via email), the preprocessing would have to be redone every single time, always with the chance that there had been changes in the layout. Recycling data in this way could be a laborious process requiring understanding of both the source and target data formats to use the data beyond its limited design purpose. In the absence of technical savvy to render visual data machine readable, much *Excel* data was essentially trapped in the local purpose it was designed for. A further liability of using visual layout to convey substantive information was that data could be inadvertently destroyed if somebody decided to sort the spreadsheet.

6.2.7.2 Children with Access to Power Tools

Microsoft *Access* was used by far fewer personnel, but where it was used its impact could be significant. *Access* puts tremendous adaptive design power in the hands of the user. Unlike other *Office* tools where a user could just create a new file and get to work, an *Access* database requires preliminary design work to create tables and forms for data entry, and unless the application is just a personal data manager, the designer also has to convince and train other people in the organization to use it. The designer would typically be somebody in a work center who just happened to have some *Access* proficiency. Examples could be found from managing personnel information to sensitive intelligence.

Design quality varied dramatically. *Access* provides numerous "wizard" tools to lower the technical barriers for novices as well as sophisticated relational database and scripting tools for advanced developers. For the latter this provided a powerful means to work around IT policy restrictions on deploying new executable programs because sophisticated code could be considered "just an *Access* file." It also guaranteed that other people would have a compatible platform to run the new application since everyone had Microsoft *Office*. However, as savvy programmers were few and far between in military organizations, most *Access* users created databases without understanding database design principles, which is not a trivial part of computer science. Enthusiastic novices could get their projects up and running in a short time, delivering noticeable efficiency gains for local data management problems, but such amateur

projects often had severe technical flaws: poorly normalized data models, "back end" data entangled with the "front end" user interface, unconstrained data entry, unreadable and unreliable code, *etc.* As a result, amateur projects became highly dependent on their designer to maintain and support, and perhaps even to populate with data if other users could not be persuaded (or ordered) to do so.[35]

Amateur projects also tended to be difficult to scale up with greater volumes or complexity of data. By virtue of their power to organize data and the enthusiasm their designers typically brought to their projects once they discovered this power, *Access* projects could easily become data traps or "stove pipes" that supported a particular small application but could not be combined with other data stores without considerable technical knowledge and effort. Moreover, *Access* data was often entered manually rather than linked or imported from another source, which created great potential for divergence, redundancy, "fat finger" error, and loss of provenance metadata. The powerful application-design potential of Microsoft *Access* provided work centers who happened to have an "*Access* guy" a way to realize real data management efficiency gains, but at the cost of becoming dependent on a designer sure to rotate out of his position in a matter of months and an amateurish design that was difficult to scale up or integrate with other information processes.

6.2.7.3 Database Incompatibility

Many of the problems which plagued *Access* projects had nothing to do with the Microsoft tool itself but were endemic to any database application in a complex organizational environment. Disconnected databases can store duplicate data, but slight differences in data model definition or data practice complicate their recombination.

Duplicate databases could emerge as small-scale groups opted to start their own data projects rather than contribute to public data stores. Most enterprise databases—to include any *official* intelligence or command and control database—protect their data models and data integrity by restricting client access to a "front end" query interface, often through a web

[35] One Army battalion S2 (intelligence officer) enthusiastically describes the efficiencies gained from keeping his intelligence data on *Access* rather than *PowerPoint*. However, he also confides that because he couldn't convince other battalion personnel to populate it, instead he had his soldiers scour the share drive to populate the database. Thus the share drive was the active "database" for the battalion enterprise, while the *Access* project was a derivative representation to support a specific shop. Michael A. Raymond, "COP: Fusing Battalion Intelligence," *Fires Bulletin* (January-February 2008): 29

browser. If users want to use some of this data for an application the client interface doesn't support, it typically takes a lot of technical and policy coordination over "data ownership" among different organizations to connect, especially if the user desires to update the data. Some data models are proprietary commercial software. Faced with organizational and technical barriers to connecting databases, the small group starts a new database to make progress on immediate needs. While the technical barriers to connecting extant data-sources can be high, at the same time the technical barriers to starting afresh continue to decline. As with the *Access* "wizards," many tools feature some database component (*Analyst Notebook* for network diagrams, *FalconView* or Google *Earth* for geospatial data, *Cold Fusion* for web application design, *etc.*), which enables a work center to begin populating a local database upon which it can become dependent.

Throughout the U.S. intelligence effort supporting operations in Iraq, data was duplicated by amateur and professional database developers alike, firstly because they couldn't access the original database or didn't know it existed, and secondly because it was so easy to start something new. In the process of local defection from contribution to shared databases, personnel inevitably defined data models slightly differently in order to accomplish their particular task with "the same" data. These differences frustrated the combination of different databases at several levels of inconsistency: (1) syntactic data format, as in phone numbers stored as 617-253-0123 vs. 6172530123; (2) semantic data format, as in feet vs. meters; (3) variant spellings, foreign transliterations, and acronyms; (4) primary keys or universal identifiers for data records, which were often just locally-generated autonumbers in the absence of standards like a Social Security Number; (6) data provenance, whether sources were included or data was just entered as a naïve fact about the world; (7) definition of database schema, as in a flat table listing bombing events by group vs. relational tables of bombings, groups, and suspected associations.[36] All of these inconsistencies created barriers to database combination, which meant that local data warrens persisted and that the combinations which did occur often compromised data integrity in the process. As we have seen repeatedly, the embodiment and format of information often got in the way of its content.

---

[36] A useful discussion of database model integrity in the context of false negatives and positives in counterterrorism data mining is found in National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment* (Washington DC: National Academies Press, 2008), 35-41.

6.2.7.4 Miscellaneous Attraction

Another common database challenge involved free-text fields, which had names like "Significance," "Description," "Comments," "Miscellaneous," "Memo," or just "Text." These fields—as with the spreadsheet formatting mentioned above—are useful for humans but do not easily support the kinds of operations a computer database is optimized to perform: sorting, comparing, and counting well-defined values across discrete records. "Well-defined" was a matter of a database working efficiently for particular needs; inevitably users come across situations that were not considered at design time, and so, anticipating this, designers provide the "miscellaneous" field to allow users to editorialize.

Often some of the most interesting data ended up in this field because users noted peculiar characteristics of a record that didn't fit in the categories defined in the other fields. The challenges arose later when one wanted to perform some aggregate operation on this irregular, semi-structured data. Free-text fields could even become an opportunity for second-order design as users started regularly entering types of data not tracked explicitly in defined fields (e.g., say some unanticipated policy concern leads users of a database which described targets to start tracking anticipated reconstruction costs for each target or categorizing targets for various strike options). Sometimes users would start inventing their own delimiters within text fields for regularly recurring data that needed a structured bucket (*e.g.,* a single field for "number of people" might see the introduction of data like "4xUSSOF|8xISF" to differentiate US and Iraqi personnel"). These emerging data-structuring norms were a form of design. Data entry in such cases could be constrained only at the informal use level or formal policy (vice in the technical database design), leading to the previously discussed challenges in data coding consistency and aggregate operations.

6.2.7.5 Collaboration Tools

Another class of application facilitated real-time multi-user collaboration. Video-teleconferences (VTC) occurred regularly, allowing commanders and analysts to meet without having to travel. The VTC tended to promote a somewhat formal and ritualized meeting style in the presence of unknown numbers of "lurkers" viewing the proceedings but not pictured on screen. The existence of VTCs also tempted administrative commands (ADCON) to try to join into operational discussions which they had no formal stake. Similarly, online chat rooms were populated by more users than had a direct role in the topic. On more than one occasion during

kinetic missions where Predator pilots and Task Unit representatives were coordinating overhead surveillance via chat, an excess of chat room voyeurs caused the application to drop mission critical participants. Lowering the costs of collaboration also lowered the costs of interference from observers (lurkers) who wanted to participate simply because they were curious.

6.2.7.6 Specialized Military Applications

The SOTF also had esoteric military-specific tools or military-unique uses of the familiar tools for operational planning, intelligence analysis, communication, logistics and administration. Compared to what might be found in other military organizations with more sophisticated weapon systems attached—an Air Operations Center, an artillery fire control center, a submarine, a nuclear command post, *etc.*—the SOTF was not as dependent on these. One expensive custom built system—the "Command Post of the Future" (CPOF)—was supposed to manage all the data in the tactical operations center (TOC) and make it easy to share with other echelons. There was an entire corner of a table dedicated to the elaborate multi-monitor system, but I never once saw anyone using it. The more technical the staff section the more likely there would be custom applications. This was especially true of intelligence, where specialized systems facilitated cryptology or imagery analysis and human intelligence management.

An important military-specific yet general-purpose application that received regular use for geospatial mapping applications was *FalconView*. *FalconView* provided a flexible platform for creating innovative small scale applications to display and manipulate geospatial data.[37] The commercial Google *Earth* application was also starting to receive some use, as the National Geospatial Intelligence Agency (NGA) had recently begun to stream classified imagery data over the SIPRNET, as Google had been doing for several years with commercial imagery on the

---

[37] *FalconView* emerged as a user innovation—written by and for pilots—in the Air National Guard and Air Force Reserve aviation community. With only a modicum of institutional support, *FalconView* inspired and competed against a series of official Air Force procurement programs. While the latter became entangled in red tape, *FalconView* diffused through user networks to become the *de facto* standard for geospatial information processing across the military services. Its extensible interface provided a toolkit for these diverse users to further customize *FalconView*'s functionality, which expanded its diffusion compared to more cumbersome and expensive purpose-built procurement programs. Whereas *FalconView* is a success story for military innovation, this study of SOTF staff work examines the converse coordination problems that emerge with pervasive flexible information tools. The history of *FalconView* is narrated in: Jon R. Lindsay, "War upon the Map: User Innovation in American Military Software," *Technology and Culture* vol. 51, no. 3 (2010): 619-651.

internet.[38] Like *FalconView*, Google *Earth* also provides a platform for further innovation to extend the application's functionality, yet the latter is far better suited to creating applications that enable data sharing across the network. An example was an overlay created by a Marine Corporal that automatically displayed icons on a map for human intelligence messages based on locations that were cited in the report.[39] A similar application was written (also by a Marine) to do the same for *FalconView*, but it required more human intervention to update. As *FalconView* and Google *Earth* had different geospatial data formats, overlays constructed for one were not easily viewed on the other.

The SOTF's data environment was a dense ecosystem of different representational tools. Those receiving heaviest use included tools familiar to information workers everywhere such as web browsers, photo editing tools, and especially the Microsoft *Office* suite.[40] Specialized military and intelligence applications had their niche, but were rarely used anywhere near their full capacity. All of these generic or specialized tools managed some subset of the SOTF's data, with a great deal of duplication and fragmentation among them. While often not technically interoperable because of data format, definition, and connectivity issues, these data traps were nevertheless operationally interdependent.

6.3 Sociotechnical Applications

The previous sections addressed interactions with specific IT. This last section covers patterns of interaction not limited to particular tools, but making use of various organizational processes. The connectivity of computer networks, the interoperability of data stores, the decisions to use particular representational tools in particular ways, all involved varying degrees of cooperation and conflict among organizationally-situated actors and all were afflicted by a

[38] User innovation has no uniform or national allegiance, as Google Earth also provides a useful planning tool to insurgents with access to the internet: Thomas Harding, "Terrorists 'use Google maps to hit UK troops'," *The Telegraph* (13 January 2007).

[39] This corporal was skilled in the Python language and created a powerful customized tool. He was relieved by another Marine who did not understood how the code worked, but could use it to produce updated products, which were emailed out to a distribution list. The tool remained static.

[40] That such tools are used as heavily in an operational staff environment as they are in managing a corporate product line or a church fundraiser testifies to the ongoing convergence of military management with civilian office work, a trend Morris Janowitz identified decades ago: Morris Janowitz, *Sociology and the Military Establishment, Revised Ed.* (New York, NY: Russell Sage Foundation, 1965)

persistent tension between authoritative design and expedient adaptation. There was no neutral technology layer within an organization; social structuration went all the way down.[41]

6.3.1 Battle Rhythm

Daily and weekly routines in wartime units are known as "battle rhythm." This ironic phrase juxtaposes the chaos, danger and uncertainty of combat with the order and predictability of routine. Yet this is the essence of military administration: rendering violence manageable. Battle rhythm generally referred to the schedule of staff meetings and deliverables.

6.3.1.1 Forcing the Update of Representations

The regular tempo of briefings set the pace for the production of many representations, acting as a forcing function to gather data and track tasks. Because the data was usually presented as a *PowerPoint* brief, the slides themselves often became the primary repositories of the data presented. A standard daily genre internal to the SOTF was the commander's (or battle) update brief (CUB or BUB) each afternoon (The SOTF operated on a late schedule, running from about noon to three in the morning to accommodate nocturnal operations). Each staff section (admin, ops, intel, *etc.*) would update their slides on their current and planned operations and present them to the SOTF commander. There was no systematic effort to save daily copies, so information presented each day was ephemeral. This minor issue would of course have been easy to address, simply creating a daily archival copy, but it highlights the sort of inadvertent design decisions that are made all the time.

Several regular weekly meetings set the tempo for coordination across staff sections. Internally, these included a targeting meeting reviewing priorities and intelligence (next chapter) and an "effects" meeting focusing on civil affairs and tribal engagement. Both meetings featured matrices of iterated activities (targets, civil affairs projects, psychological operations initiatives) listing their readiness status (in red, yellow, green "stoplight" charts) and other pertinent data. Many staff officers maintained their tracking information directly on their briefing slides, allowing the briefing requirement to constrain their operational data tracking. Some staff members cut cells of data from *Excel* spreadsheets and paste them to fit on a *PowerPoint* slide, which often led to a divergence between slide and the spreadsheet as errors were detected and

[41] Wanda J. Orlikowski, "The Duality of Technology: Rethinking the Concept of Technology in Organizations," *Organization Science* vol. 3, no. 3 (1992): 398-427

fixed directly on the slide in order to get ready for the brief. Such tedious little matters tended to take up hours simply preparing *PowerPoint* slides.

6.3.1.2 Post-Hoc Guidance

Task Units were on the hook to provide some slides for SOTF staff officers to brief the commander, and they perceived these weekly deliverables as taxes that provided information to the SOTF staff but provided little in return to assist actual Task Unit targeting and engagement activities. SOTF staff officers on the other hand used the brief as a tool to extract information from the Task Units that they might not have readily shared ("I need it for the skipper"). These presentations were often framed in terms of directing SOTF guidance to Task Units and tracking their progress, yet often this guidance seemed more of a retroactive rationalization of what the Task Units were inclined to do anyway: "This is what we're doing now, so this is also what we meant to do before."

6.3.1.3 Re-Reporting

One of the most important written genres in military organizations is the daily situation report (and for intelligence organizations, the daily intelligence summary). The report describes a unit's operations over the past twenty-four hours, planning priorities for the future, logistics conditions, requests for support, *etc.* At the SOTF these were produced at the lowest levels—SEAL Platoon or Special Forces Team—and forwarded up. These were consolidated at each level, cut-and-paste into a *Word* document, with additional comments from the commander (rather, his staff) appended at each echelon. By the time the SOTF's higher headquarters released its report, it might be eighty pages long! It would also be delayed by the editing time of several hours at each echelon. SOTF operations officers would then have to scan the higher echelon situation report to see whether their own reporting had been changed or commented on. Many staff products that appeared to be unique or promise some value-added were in fact just aggregated reproduction of other units' reports.

6.3.1.4 Different Formats for Different Masters

A set of weekly meetings revolved around a set of *PowerPoint* slides known as "quad charts" presenting a 2-by-2 matrix of mission objectives, targeting, engagement, and intelligence overviews for each Task Unit and the SOTF as a whole. The SOTF prepared these for its operational (OPCON) commander in Bahrain and presented them in an online conference session (referred to by the application's name "Click-to-Meet"), which required an additional meeting

before the meeting among the SOTF and Task Unit commanders. These slides were then recycled as notes used by the SOTF commander in a weekly video-teleconference with the tactical (TACON) commander in Balad. The quad charts recapitulated information in the daily SITREPs and in the weekly targeting and effects meetings. But as it was desired in a slightly different format, and thus with different degrees of summation, it became an additional production requirement. As with so many applications discussed above, this led to multiple redundant data stores, with a lot of manual formatting, repackaging and synchronization work required. Each product was used in a different genre, coordinating slightly different types of activity and audiences. Many hours of staffwork were consumed reformatting the same information in different ways for different purposes.

6.3.1.5 Work-to-Rule with Administrative Requirements

Some product cycles had lengthier timelines: monthly reports, preparation for turnover for the next squadron, award submissions, periodic personnel evaluations, *etc.* The timing of the squadron deployment exerted a change in personnel attitudes. Take awards for example. Medals have long been a means to motivate military personnel to strive and to sacrifice by visibly rewarding them for courage and effort. While there are indeed still awards issued for exceptional individual acts, the process has also become somewhat ritualized, with an expectation that awards shall be presented to each individual at the end of each deployment (as well as at the end of each tour). Thus the SOTF began requesting Task Unit inputs for end-of-deployment awards when they were only four months into a six month tour. As personnel turned to writing awards, drafting fitness reports, preparing turnover material, and other bureaucratic requirements for returning home, they paid less attention to thinking innovatively about the warfighting problem they faced. Given that it took SOTF units about a month to get into an effective rhythm when they first entered into theater, thus only really three months out of six were productive (or reflected in a "deployment award").

6.3.2 Offloading Aggregation

Asking for new products is easy, but aggregating across existing ones for new purposes is hard. When staffs did not have information in a format that easily afforded answers to their questions, they often requested data from their subordinate units in a new format. The tragedy is that the headquarters often had the information, but was unable to access it because it was not

recorded in an accessible way, given the skills and disposition of staff personnel. The organization didn't know what it already had, so it asked subordinates to report anew.

An example was a weekly "by the numbers" brief that each Task Unit sent to the SOTF each week listing totals of each category of mission it had executed.[42] An *Excel* spreadsheet maintained by the SOTF tactical operations center (TOC) could easily have been queried for this data, but Task Units were nonetheless required to report tallies in a *PowerPoint* slide (because TOC personnel didn't understand how or were unwilling to use *Excel* cross-tab queries). The headquarters had the ability to aggregate in principle, but had difficulty spanning and aggregating its own pools of information, so it offloaded the task to the Task Units. This particular example seems trivial and easily correctable, but similar instances could be iterated *ad infinitum*. Staffs could only really answer questions based on the records they collected, and in the format they collected them in. New questions that came down the chain of command didn't fit the records.

The Task Units had nearly twenty different kinds of daily and weekly regular reports due to the SOTF,[43] as well as endless one-off calls for information. Requests for information from the SOTF or its headquarters (or headquarters' headquarters, or...) were usually pushed down to the Task Units and from there to the platoons. Forward units—those with regular contact with Iraqis—were constantly hit with new data calls to provide some additional type of information, or more detail on something already submitted. Often the new requirement would specify the format of the data: a new matrix or map, usually a *PowerPoint* slide. While each product might include some unique information or useful presentation, there was also a great deal of overlap between all the products. Reporting units invariably generated each new product manually. The administrative load was reproduced at each echelon as products were aggregated and sent

[42] Missions could be categorized as routine convoys requiring only Task Unit approval, targeting missions requiring SOTF approval, or very sensitive missions (like mosque entry) requiring CJSOTF approval. This mission level would be recorded on a SOTF headquarters *Excel* mission tracker at the time of mission execution. In addition to their approval level, missions also could be categorized by their purpose: a convoy could be a supply run, a coordination meeting with Marines, a tribal engagement event, or a HUMINT operation. These totals by mission purpose could have been tracked by SOTF staff officers in different ways, by counting engagement or HUMINT reports, for example. Instead Task Units were queried to provide summary statistics.

[43] A daily situation report (SITREP), draft and final concepts of operation (CONOPS) for missions, target intelligence packages (TIPs), "Click-to-Meet" quad charts, after action "quick looks", after action "storyboards," CUB slides, training statistics, training photographs, intelligence reports, engagement reports, civil affairs packages, casualty reports, *etc.*

forward, with only the lowest levels usually providing any original input. The tragedy was that many calls for information could often have been answered in part by looking across existing product lines. Headquarters staff members, either not understanding the existing reports, or unable to figure out how to technically sift through the data themselves to identify any genuinely novel residual requirement, or simply lazy, tended to levy new reporting requirement on lower echelons in their entirety. To deflect complaints, staff officers typically put the blame on the higher headquarters ("CJSOTF is making us do it") but levied the tax nonetheless.

Robust network connectivity increased the reporting burden on lower echelons. Clausewitz points out that reporting from the field is always partial and contradictory, but now with the ease of communication it is possible to demand more information to try and fill out that partiality and attempt to resolve the contradictions. The claim is often made that digital networks improve situational awareness about local areas for anyone on the network. However, someone has to type that information into the network. The lower echelon units, the SEAL platoons and SF teams, were busy with maintenance, training, intelligence, operations, as well as drafting reports about all this activity. It was not possible to both do everything and to write about everything in detail. Thus there was still much to be learned about what a unit was doing by actually visiting it in person, rather than simply reading reports.

6.3.3 Reach Back

Organizations in the continental U.S. attempted to exploit IT connectivity to relieve forward units of some information processing. In principle "reach back" (outsourcing) provides information products and services without exposing producers to danger or expanding forward footprints in combat zones. Reach back can also co-locate intelligence support with agencies in the U.S. Eastern Time zone to exploit daylight working hour coordination.

Despite the existence of a lot of reach back support organizations, the SOTF (and the Marines) still produced most operational information products in house. The same connectivity that made reach back work in principle also delivered most of the same source information to analysts in the field, so they could do the work themselves. While reach back provides more manpower, it does not necessarily provide any more information sources or computational power. Moreover, the reach back analysts lacked the tacit, situated sense of what intelligence customers required, something that comes from working eighteen hour days for months on end

in an operational environment. This demand-side information is "sticky" and difficult to articulate.[44] The customer is faced with a choice between on the one hand explaining at great length was he needs in order to take advantage of reach back manpower, taking a risk that the requirement might not be understood or might change before delivery, and on the other hand just doing the support project on site. For the types of intelligence problem where more manpower might help—careful targeting analysis or in-depth tribal background studies—deployed customers were often suspicious that reach back analysts were too far removed from downrange concerns to provide timely and relevant assistance. To complicate matters, the telephony problems described earlier frustrated ready secure voice communication between the SOTF and support at ONI. There appeared to be two conditions under which reach back could work.

6.3.3.1 Standardized Products

First, if the product was extremely stereotyped, then both sides could know what to expect. The NSW Mission Support Center (MSC) provided standardized target objective area studies with richly annotated imagery.[45] SEALs trained with these during their work up and knew what to expect, and the MSC could turn them around in a matter of hours. This could be of great assistance to well-understood mission profiles.

6.3.3.2 Close Personal Relationships

Second, if the individuals on both ends of the relationship had a great deal of shared experience and a prior face-to-face relationship, then they could save a lot of time in communication by anticipating one another's needs. The reach back analyst could empathize with the customer's situation and the customer could trust the analyst not to waste his time with superfluous queries. One example was an individual who had recently redeployed from the SOTF where he had first-hand experience as an interrogator, providing reach back support from the Office of Naval Intelligence where he could aid in the analysis of several complicated interrogation cases. Thus, reach back support had to either be a standardized arms-length

---

[44]Eric Von Hippel, ""Sticky Information" and the Locus of Problem Solving: Implications for Innovation," *Management Science* vol. 40, no. 4 (1994): 429-439

[45] Given the location for an assault objective, MSC personnel would find a recent satellite picture and annotate on top of it in different colors all the doors, windows, height of fences and parapets, and potential "squirter routs" where people on the objective might flee. This could be turned around within a few hours (or less) of a request. The product was completely stereotyped. The producers didn't have to know anything about the target; they just needed a set of coordinates to access imagery—which collection and distribution architectures stabilized in order to guarantee that the image was of the given coordinates—so they could start annotating.

transaction, or an extremely personalized interaction, otherwise the ambiguity and context-specificity of the intelligence problem tended to generate prohibitively high coordination costs.

6.3.3.3 Reach Back Supported "Kinetic" Missions

Reach back support tended to be biased toward supporting the targeting missions. There were more resources available for tracking and targeting insurgents. This may simply have been a matter of demand: when the supported organization prefers targeting, the supporting organization will indulge. There may also be similar biases on the supply side. Supporting targeting is more dramatic and allows reach back analysts to vicariously live through the SEALs they are supporting. The creation of large well-funded stateside outfits like the Joint Improvised Explosive Device Defeat Organization (JIEDDO) also creates supply-side slack that enterprising customers can coopt for their own purpose if they can tie their mission to combating the IED supply chain (which includes almost any insurgent activity). Yet there appears to be an additional informational reason channeling the bias toward targeting support. If reach back works reliably well for standardized products and if targeting involves a lot more standardized operating procedure (as discussed in the previous chapter), then they are well suited for one another. Indirect action, engagement, and persuasion missions, by contrast, involve a much greater degree of complexity and ambiguity, and the likelihood of having both sides of the reach back relationship conversant in this realm is comparatively lower. Reach back amplified the targeting capacity of the SOTF, but at the cost of neglecting other types of support.

6.3.3.4 Vicarious Frogmen

Reach back was often pitched in terms of "support to the warfighter." This allowed organizations in the extreme rear to vicariously claim some association with ongoing combat operations thousands of miles away. *PowerPoint* briefings could "show" how intelligence support was directly facilitating forward operations, activity usually too remote or too secretive for briefing audiences to follow up on whether the support actually had the advertised effect.[46] Briefing presentations and impressive computerized visual displays provided dramatic content for funding requests or other types of patronage. A perverse consequence of such bureaucratic incentives is that reach back organizations often ended up demanding that information flow in the opposite direction, from the field to support the domestic promotional performance. This

[46] I have seen several instances of circumstantial correlation without real intelligence causation passed off as supposedly decisive reach back support

tension would be most acute when the reach back organization actually had an administrative (ADCON) relation to personnel in the field and could thus levy additional reporting requirements. Reach back could just as well be called "reach forward."

6.3.4 Classification

Chapter 5 touched on the fragmenting effects of classification policy. Rationally this tradeoff protects sensitive sources and methods which would be compromised by enemy knowledge. The tradeoffs between "need-to-know" and "need-to-share" are eternal with classified information, and friction is unavoidable. Some of this classification-induced friction had an interestingly social aspect.

To move information across "air-gapped" networks, people used removable media such as floppy disks, memory sticks or "thumb drives," or portable hard drives. A battery of prophylactic security procedures regulated movement (text-scanning the media for "dirty words," review by two people, creating read-only CD-ROMs, *etc.*), but these procedures were often more honored in the breach as personnel expediently moved from one operating location to another. The use of thumb drives was ubiquitous in Iraq even though SOCOM had recently restricted their use because they had become a vector to compromise data and to introduce internet viruses to classified networks.[47] It is hard to evaluate whether the security gains of the ban were greater than the net efficiency loss imposed on responsible users trying to cope with the fragmented nature of their networks.

Paper printouts also provided a low-tech means of liberating information from classified systems. Just as thumb drives were used to work around classification barriers, users would print out information from classified systems that might not itself be classified as highly. The pages could be filed or circulated, including giving unclassified documents to Iraqis or the press.

---

[47]Paul Watson, "U.S. Military Secrets for Sale at Afghan Bazaar," *Los Angeles Times* (10 April 2006); Noah Shachtman, "Under Worm Assault, Military Bans Disks, USB Drives," *Wired* (18 November 2008). The thumb drive virus which ultimately led to the ban was a sophisticated "social engineering" virus which exploited the propensity of users to disregard security barriers and use the drives to transfer data. This mechanism could be used not only to insert malicious performance-degrading code onto classified networks, but also to exfiltrate data payloads out from classified systems across air gaps. Thumb drives infected with such viruses could be left where users might happen to purchase them—say while on patrol in a bazaar—or just as likely viruses might be uploaded with pornography which, despite unambiguous policy prohibitions, seemed to find its way onto the SIPRNET. Thumb drives with secret information and personnel data on US soldiers have indeed turned up in Baghram bazaars

Rather than comply with the nuances of official classification guidance, many users simply classified their work at the highest level of the system they were working on. Nobody wanted to have a security violation in their record to adversely affect their clearance eligibility. Reflexive over-classification was especially likely with email because of a required Microsoft *Outlook* add-in function that forced personnel to classify their messages before sending; most users simply set a default high level for convenience. Because SIPRNET was the standard working environment, this meant that even routine administrative correspondence was regularly over-classified "SECRET/NOFORN", which is not releasable to allies and is unlikely to be declassified for a decade or more.[48]

Because it was easy to create new digital documents yet hard to verify the proper level of classification, users produced a flood of information which had to be handled at the highest level. It is difficult to estimate how much information marked as classified on any particular network was actually classified at that level (or classified at all), but it was probably not insignificant. What if slides had to be shared with allies, uncleared visitors, or moved to an unclassified network? Again this resulted in security regulations being more honored in the breach as people made contingent judgments about how to handle or release information at their local level, thus undermining the protection that such classification marks were intended to provide.

Classification practice created boundaries around information in order to protect sensitive sources, methods, and operations, the compromise of which could imperil national security and the lives of servicemembers. Boundaries could serve other purposes, however. Personnel often took classification as a proxy for information value: the higher something is classified, the more useful it must be. This correlation is a fallacy. An overt tip from some local tribal person could be more actionable—leading directly to capturing an insurgent—than TS/SCI intelligence. An analyst might invest dozens of hours creating a fancy visualization of data from a highly classified sensor which provided, however, little "value added" beyond an exhibition of the sensor's capabilities and the analyst's technical wizardry. The conflation of classification with

[48] A mundane message in an intelligence shop like "Sergeant Jones will be collecting Toys for Tots donations today" could routinely end up classified "TS/SCI," which technically means "the unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to national security"! Classification guidance makes a distinction between original and derived classification. Original classification authorities reside with specific agencies. Derived classification depends on the highest level of originally classified information which is included. Users were essentially acting as *de facto* original classification authorities by classifying everything they produced.

value led to several dubious assumptions: people who have access to it must be doing valuable and interesting work; it is worth going out of my way to get access to it even at the price of neglecting work with known pay off; there is probably information that is valuable to my job that I am not cleared to see; higher prestige organizations have better information. There was a voyeuristic appeal around highly classified information, such that those who were able to, one way or another, wanted to get a peek.

Classification thus became an in-group marker. Those who were "read in" to a program were in the club, excluding those who were not. Classified information could then be dispensed as a form of patronage, delivered in conspiratorial whispers, regardless of whether either interlocutor was actually cleared for the information. The dissemination of information then became a matter of personal networking rather than impersonal bureaucratic control. Such "secret squirrel" hoarding could impede information exchange even between people who had an ostensible need to know. *Ad hoc* meetings in the SCIF were often a who's who of the SOTF social hierarchy, helping to reinforce who was "in the loop" on important information, whether it was classified or not. Those who were excluded from the meeting because of a lack of credentials assumed that important, mission-critical matters were being decided, even though such meetings were more often than not strictly informational. The attitudes of those in the out-group reinforced the exaltation of the in-group as much as the actions of the latter.

Classification imposed boundaries on the flow of information. Some of those were legitimate for the protection of security, some were created with the ease of labeling ever more digital documents, and some more perversely enhanced social prestige. Because the latter uses were personalized, they could be difficult to recognize and penetrate. Surely there was far more classified data than a rational justification of need-to-know would allow for.[49]

6.4 The Interference Variety of Information Friction

While it is perhaps amusing to see some of the same IT foibles in this rarified setting as in office cubicles anywhere, it's also disturbing once we also consider that the SOTF's cascades of inscription connect *PowerPoint* slides to lethal battlefields. Many of the coordination problems documented above could have been abated by personnel with a little more technical savvy and sensitization to the externalities of IT coordination, reliability, security, and

[49] Peter Galison, "Removing Knowledge," *Critical Inquiry* vol. 31 (Autumn 2004): 229-243

scalability. More and more personnel spend more and more time with these tools, but they are like soldiers who don't know how to operate their weapons. Their effort is often wasted on self-inflicted digital wounds and fratricide which, unlike the real thing, they feel only dimly. Remarkably, technical incompetence—as well as the mundane genius which helps to clean up its mess—remains largely invisible and somehow acceptable to modern IT-intensive forces. We have seen recurring negative externalities emerge with tool after tool, in support of many different types of mission, iteration after iteration of work processes. This background noise should be expected in any IT-intensive environment, but in the SOTF it could sometimes become deafening.

6.4.1 Manual Effort to Support Automated Processes

In general, human beings provided the bridges between applications and specific representations, manually reprocessing or even retyping data. If a new format was required—say someone wanted an *Excel* spreadsheet based on data in templated *PowerPoint* slides, or a specialized military application required data to be typed into a database—usually some unfortunate enlisted clerk or junior officer would be assigned the tedious job. While it might in principle be feasible to automate the extraction of the data (e.g., parsing *PowerPoint* data into *Excel*), in practice very few personnel had the technical savvy to write scripts or macros to automate portions of such data-transformation. In rare cases where a user did have the technical wherewithal to pre-process and consolidate data, then the shortcuts were generally only used by their creator since regular tinkering was needed to deal with inevitable changes in format and context that cropped up in subsequent iterations. The flexibility of scripting tools from the perspective of the script-writer became brittleness from the perspective of less technically-inclined users. Thus even where data processes could be automated with user scripts or new purpose-built applications, there were always users struggling to work the seams of their fragmented information environment.[50]

Human activity was critical for system interoperability, whether reprocessing data by individuals or "knowledge management" policy regarding file and folder naming conventions and portal population by organizations. Human interaction with and across applications was a

[50]Greg Downey, "Virtual Webs, Physical Technologies, and Hidden Workers: The Spaces of Labor in Information Internetworks," *Technology and Culture* vol. 42, no. 2 (2001): 209-235, characterizes this type of interoperability labor as "boundary work" which is largely invisible in the operation of networks.

necessary part of the entire representational process. Computer architectures are designed in layers (hardware, operating system, application) and thus often think of the "user interface" as simply the way the user perceives and interacts *with* a particular program at the "top" layer. By contrast, what we see here is that users also provided the interface *between* applications at many different layers. A further manifestation of representational fragmentation was that most users at any one time would have many different windows and many different applications open at any one time. A few users had multiple monitors to view several windows at once while most others had to cycle through windows one at a time. Both styles involved users frequently switching attention among applications and document in order to cross-reference, multi-task, and cut-and-paste. This was simply a visible manifestation of the interoperability work users performed.

None of the specific challenges described in this chapter were in themselves technically intractable. Once recognized and understood, there was usually in principle a better technical solution for the data management challenge at hand. For instance, the use of *PowerPoint* template slides "as if" they were a distributed database could certainly have been replaced with an actual relational database to improve referential integrity and the efficiency of aggregative queries. Such recognition and understanding, however, is not trivial, and in every case has to be worked out or debugged in practice. Alternatively, commonly available tools—providing affordances for adaptation in the absence of technical savvy—made it easy for personnel to default to expedients. Thus, while the technical problems might not be insoluble, the daily grind of identifying and working through them was unavoidable, and it contributed to the general background of friction afflicting day-to-day military operations. Information does not float freely; it is contained, both intentionally and not, within a myriad of different pools and channels by physical and organizational structure. It took ongoing technical and political effort, sometimes within the rules and sometimes around them, to make this infrastructure work.

6.4.2 Centrifugal Fragmentation

Chapter 3 described how "centers of calculation" support the combination of incoming cascades of inscription to create more abstract and powerful representations of the world. Throughout this chapter we have seen how these centers sprang up all over the place, in multiple workcenters and in multiple applications on the same work center. In radical contrast to the material centralization of physical maps and plotting boards—like the type described in the

Battle of Britain study—individual users were empowered to start up their own fusion sites willy-nilly (de-centers of calculation?). They could make new folders, copies of files, and copies of data in new files. Usually they did not articulate the assumptions that went into their constructions, and they threw away provenance data along the way. Modern IT promoted a decentralizing effect even among personnel working in the same room. While it seemed sensible at the time for each user to pioneer idiosyncratic processes, the result was a fragmented mess.

Organized files and populated portals are a public good. Individuals often stopped contributing their share unless they were forced to. Yet even hierarchical pressure could not adequately monitor and enforce local practices, simply because the technology was so combinatorially rich for individual users. In the SOTF, this technical affordance for bottom-up mess-making was magnified by the improvisational ethos of special operations, which also meant a reticence for superiors to question the man in the field, together with the woefully uneven level of IT literacy.

6.4.3 Friction as a Cause of Itself

Table 6-2 lists the phenomenological (experiential) and prosthetic (functional) manifestations of information friction, with a couple of examples of each drawn from the many more discussed above. IT could both lower and raise friction, and thus IF2 (attention) importantly describes the regular drift from smooth usage to wrangling with and debugging representational processes and structure. Table 6-2 does not show a clean coding of high or low friction, but rather suggests a dynamic of personnel trying to work through it and generating more in the process. Information friction was constantly boiling up in the everyday processes of distributed cognition.

Table 6-2: Phenomenological and prosthetic manifestations of information friction in the SOTF

	Low Information Friction	High Information Friction
Phenomenology *(qualitative experience of participants in the information system)*		
IF25. Sensemaking	*"Situational awareness"* The organization keeps going	*"Fog of war"* Quotidian, niggling, insulated from consequences
IF26. Attention	*{actor → tools} → world* Temporary availability of world	*actor → {tools → world}* Attention regularly drawn to representational problems
IF27. Format	*Transparent usage* All tools have moments of smooth usage	*Obtrusive breakdown* Much effort spent on format, compatibility, access
IF28. Content	*Felicitous/available* "Can you email me that?" Battle rhythm forces update	*Unreliable/unavailable* Sluggish search Unpopulated portals
IF29. Uncertainty	*"Aleatory" values on variables* Regular meeting products	*"Epistemic" models & methods* Multiple folder trees The "miscellaneous" field
IF30. Politicization	*Harmony* Ritualized Battle rhythm Reachback personal relationships	*Controversy* Rhetorical products Reachback supply push Post-hoc HQ guidance
Cognitive Prosthetics *(IT usage amplifies human perception or misperception)*		
IF31. Affordance	*Suggest appropriate action* Paper for legibility, durability, annotation Slide-building collaboration	*Mask possible action* Email/portal/server data warrens Offloading aggregation
IF32. Perceptual Offload	*Reduce cognitive load* Visual layouts of spreadsheets Dual-use data/display slides	*Uncritical acceptance* Reformatting for HQ Reification of simple graphics Pasting map data to Powerpoint
IF33. Precomputation	*Spread load over time & people* Base layers of maps Slide "databases" spread load Standardized reachback	*Hidden assumptions* Idiosyncratic overlays & slides without provenance data Intellipedia
IF34. Precision/Complexity	*Sophisticated measurements* Relational databases Large-scale distributed info processing throughout SOTF	*Dependency & opacity* Interoperability/reliability Re-reporting Administrative requirements

How did anything get done? The next chapter will describe how this infrastructure was put to work for the SOTF's principal computational problem: targeting insurgents. The SOTF was a strange mix of decentralized interference and centralized insulation. This chapter revealed endemic interference in daily tool use. The next chapter shows how the strongly infused values of the U.S. special operations community amidst the counterinsurgency in Anbar promoted insulated tool usage. The SOTF's fixation on killing or capturing bad guys served to mask the friction in the construction of products which supported such activity. Methodological and intelligence gaffs could be swept away as a more heroic narrative was reconstructed in the *PowerPoint* slides about targets and raids which bubbled up to prominence. Endemic interference friction was greased over with biased insulation friction. The next chapter will trace the ways in which the same tools that might improve organizational information management could also contribute to blind spots and bureaucratic myopia.

Chapter 7: Target Fixation

"Consider your verdict," the King said to the jury.
"Not yet, not yet!" the Rabbit hastily interrupted. "There's a great deal to come before that!"
-Lewis Carroll[1]

7.1 Distributed Cognition in Targeting

Chapter 6 described information technology (IT) usage patterns in a U.S. special operations task force (SOTF) in Iraq. Flexible digital IT, uneven technical expertise, and a complex bureaucratic environment all combined to fragment information processing and preoccupy personnel with uncoordinated data management schemes. This *interference* variant of information friction generated noise for any given mission. The *insulation* variant, by contrast, causes an organization to reproduce its preferred patterns of behavior without perceiving counterproductive consequences. This chapter describes such friction in the SOTF's primary preoccupation: targeting insurgents.

While interference stems from decentralized collective action problems, insulation arises from more centralized lock-in and/or rent-seeking. How was it possible to have both decentralization and centralization in the same organization? The fragmentation of the SOTF's networks across internal staff divisions and external partnerships created a general level of noise and coordination difficulty. At the same time, a strong doctrinal worldview canalized representations in a particular direction and constrained the types of questions likely to be asked of them. In terms of distributed cognition, this composite insulation-interference friction manifested as rough agreement on the computational ends of the system with an equivocal implementation of its representational means. Although interference friction was pervasive and obtrusive, insulation friction enabled personnel to suppress it and to instead reconstruct a simpler narrative about killing and capturing bad guys. The performance of raids thus tended to mask any methodological errors in the construction of targets or unintended consequences of raids in the broader Anbari society.

[1] Lewis Carroll and Martin Gardner, *The Annotated Alice, The Definitive Edition* (New York, NY: WW Norton & Co, 2000), 112

Rather than the value-free panoptic "common operational picture" envisioned by "revolution in military affairs" (RMA) doctrine, the SOTF used IT to construct a version of its environment organized in terms of its *ex ante* preferences. The organization's technology of perception illuminated a world that Navy SEALs were predisposed to see. IT usage was not the initial cause of this bias, but it became an amplification of it. This is a case of one particular special operations unit at one particular time; that very particularity shaped the application of IT in contradistinction to simplistic RMA determination by advanced networks and Joint doctrine. This case problematizes IT usage by highlighting its potential for breakdown in social context.

This chapter begins with a description of the computational problem of targeting insurgents and then steps through the SOTF's implementation of the control processes defined in Chapter 3: perception, integration, and articulation. It closes with an assessment of battlefield performance, emphasizing the difficulty of measuring it given the insularity of the SOTF's information system. As a test of information friction theory, this case is designed to measure the causes of friction and their result (friction as a dependent variable) more than the consequences of friction for battlefield performance. The latter is obviously why friction matters, so I will call attention to the potential consequences of the information breakdowns I discuss along the way. This case problematizes human-computer interaction which RMA doctrine takes for granted.

7.1.1 What is Targeting?

Military targeting boils down to the problem of hitting something at a distance.[2] This core military task has not been examined much in security studies, in part because of its secret and technical nature, but also because it's usually considered a merely tactical job best left to professionals. The scholarly attention that has been paid to targeting has focused mainly on air campaigns and nuclear weapons.[3] There is some emerging interest in counterterrorism targeting,

---

[2] Alfred W. Crosby, *Throwing Fire: Projectile Technology Through History* (New York, NY: Cambridge University Press, 2002)

[3] Frederick Kagan, *Finding the Target: The Transformation of American Military Policy* (New York: Encounter Books, 2006), 126, notes, "The importance of theory to air power flows from the fact that the critical question in air planning is...'What should we bomb?'" On strategic bombing targeting see: Walter W. Rostow, "The Beginnings of Air Targeting," *Studies in Intelligence* vol. 7, no. 1 (1963): A1-A24; Stephen L. McFarland, *America's Pursuit of Precision Bombing, 1910-1945* (Washington, DC: Smithsonian Institute, 1995); Robert S. Ehlers, Jr., *Targeting the Third Reich: Air Intelligence and the Allied Bombing Campaigns* (Lawrence, KS: Kansas University Press, 2009). On nuclear targeting see: Desmond Ball and Jeffrey Richelson, *Strategic Nuclear Targeting* (Ithaca, NY: Cornell University Press, 1986); Kenneth T. Johnson, "Developments in Air Targeting: Progress and Future," *Studies in Intelligence* vol. 3, no. 3 (1959): 53-62.

also called "leadership decapitation," because it has become the *de facto* strategy of American counterterrorism efforts led by U.S. Special Operations Command (SOCOM).[4]

Because targeting sits functionally at the nexus of intelligence and operations—where personnel translate information coming in from the world into decisions to go out and act—it is well suited for examining the entire control cycle of distributed cognition. Thus targeting should be of more general interest for students of organizational perception. Furthermore, a central belief of RMA doctrine is that robust networking improves situational awareness, which improves targeting speed and precision. The SOTF was well-endowed with modern IT networks and access to intelligence, surveillance, and reconnaissance (ISR) assets; it was a Joint organization in that, although its Naval Special Warfare core hailed from one service, it fell more under the sway of SOCOM than the Navy. According to RMA doctrine, we should see IT contributing gains in mission effectiveness in this case. If we see information pathologies in the area where the RMA should be most effective, then we learn something about its limitations.

7.1.1.1 Manhunting

If targeting in general tries to hit something at a distance, then special operations targeting endeavors to hit the leadership of a clandestine organization with commando assault teams. It combines an expansive network of human and technical intelligence collection to cue up raids to kill or capture insurgents. Such targeting follows the logic of the hunt, in which a predator and its prey employ asymmetric strategies to facilitate or frustrate their intersection, respectively.[5] The prey tries to reduce its signature and to control its vulnerability while the hunter strives to improve acuity and access.

The hunter's control problem is to arrange a situation so that his path intersects with that of the prey. The hunter can employ *stand hunting* or *ambushing* to interdict the prey along its

---

[4] Jenna Jordan, "When Heads Roll: Assessing the Effectiveness of Leadership Decapitation," *Security Studies* vol. 18, no. 4 (2009): 719–755; Seth G. Jones and Martin C. Libicki, *How Terrorist Groups End: Lessons for Countering Al Qa'ida* (Santa Monica, CA: RAND Corporation, 2008); Daniel Byman, "Do Targeted Killings Work?" *Foreign Affairs* vol. 85, no. 2 (2006): 95-111 ; Kenneth Anderson, "Targeted Killing in U.S. Counterterrorism Strategy and Law," Counterterrorism and American Statutory Law Working Paper, Brookings Institution, Georgetown University Law Center, Hoover Institution, 11 May 2009

[5] These hunting strategies draw on the discussion in Steven M. Marks, Thomas M. Meer and Matthew T. Nilson, "Manhunting: A Methodology for Finding Persons of National Interest," Naval Post Graduate School, Masters Thesis (June 2005),19-32. See also on manhunting: David Scott-Donelan, *Tactical Tracking Operations* (Boulder, CO: Paladin Press, 1998); Ron Reid-Daly, *Pamwe Chete: The Legend of the Selous Scouts* (Weltevreden, South Africa: Covo-Day, 2001)

route of travel. He can *stalk* the prey via signs and spoor, and he can *pursue* to close the distance. *Calling* and *baiting* can lure the prey out of hiding or cause it to change course into a trap. *Flushing* drives the prey out of hiding into the sights of companion hunters who wait.

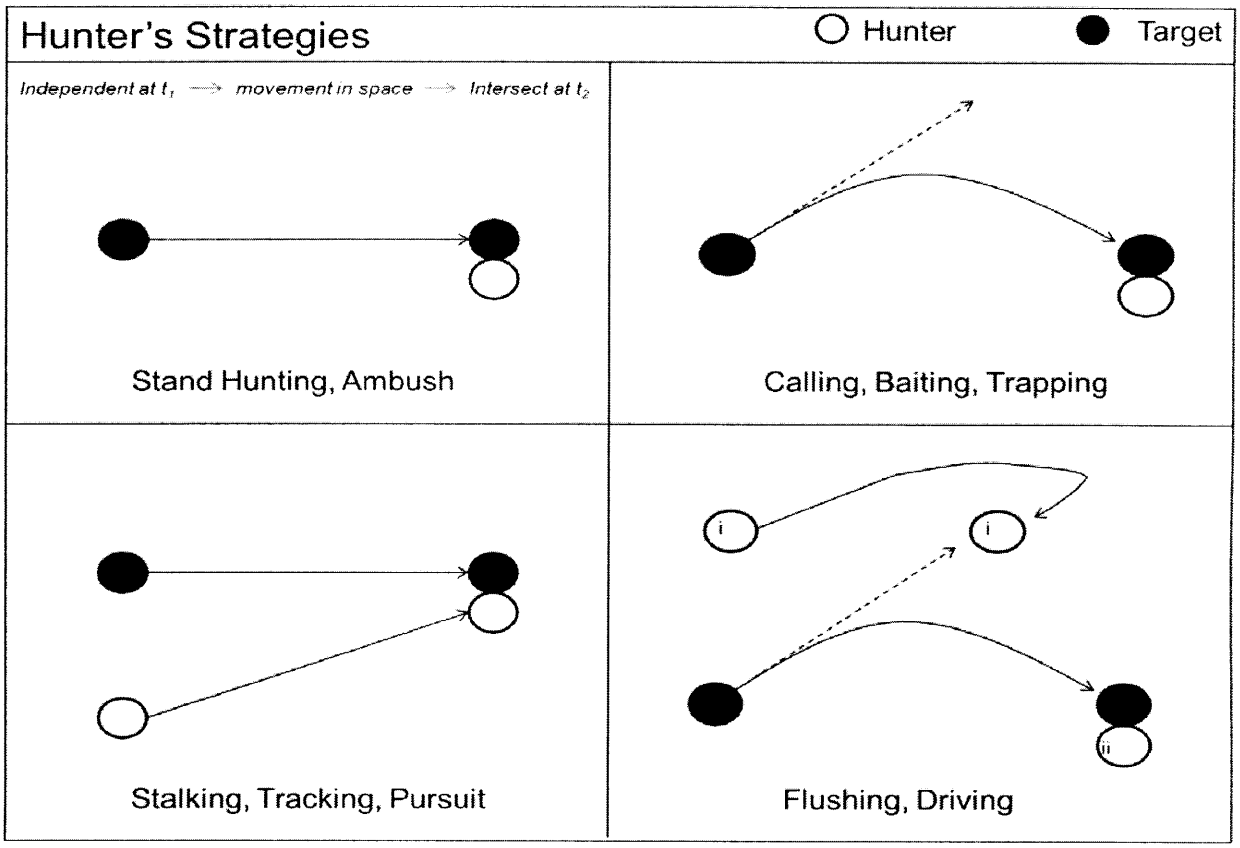


Figure 7-1: Strategies for the hunter to achieve intersection with the target

The target has strong incentives to counter the hunter's strategies because, as Richard Dawkins points out, "The rabbit runs faster than the fox, because the rabbit is running for his life, while the fox is only running for his dinner."[6] The prey employs *camouflage* or *deception* to reduce the signature it presents to the hunter. It can *maneuver* or *flee* to evade pursuit, or it can *disengage* by moving across a jurisdictional boundary into a sanctuary not accessible to the hunter (as al-Qaeda retreated into Pakistan). Furthermore, the human target has options that game animals do not. The insurgent can also choose to *ambush* or *subvert* the hunting forces. When the hunter is a foreign occupier or overbearing government, the target may actually only exist because of, and thus actively stalk, the hunting party. The hunters can become the hunted.

---

[6] Richard Dawkins, *The Blind Watchmaker: Why the Evidence of Evolution Reveals a Universe without Design* (New York, NY: W. W. Norton & Co, 1996), 191.

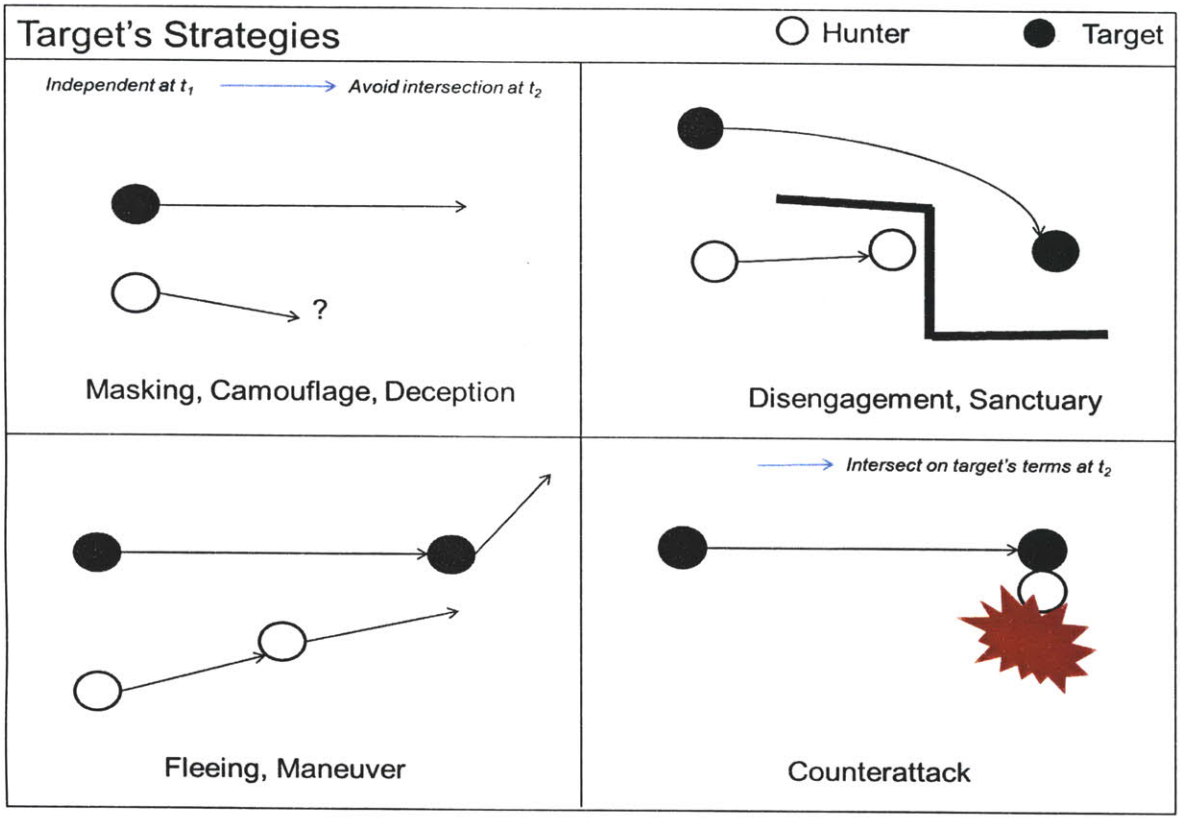


Figure 7-2: Strategies for the target to avoid intersection

Figure 7-1 and Figure 7-2 depict the strategic options and thus abstract computational problems of hunter and target. The hunter's problem is to arrange an intersection at a future time while the target's is to avoid it. Figure 7-2 does not include the critical problem of the target's identity or validity changing in the middle of the hunt; Chapter 5 discussed the challenges of fickle loyalties in counterinsurgency. In the hunting analogy, this might be like a permit expiring in mid-pursuit or the local guide transforming into a dangerous bear. The hunter's ongoing validation of the target *qua* target is thus a precondition for a successful intersection. Whatever combination of strategies each side employs, the hunter has a complicated information-processing problem to compute the future intersection. Friction in the hunter's information architecture impedes his ability to compute a connection and inadvertently assists the target's counter-strategies.

7.1.1.2 Counternetwork Operations

Special operations organizations implement the hunting strategies above by conducting iterated targeting operations. Each insurgent captured is a collection opportunity for identifying

and tracking more insurgents. A captured insurgent can provide information directly through interrogation, or captors might be able to "flip" or "double" the prisoner in order release him back into the insurgency as a spy or subversive agent. He might even serve as hostage collateral for negotiations with other insurgents, or as bait to ambush an insurgent rescue attempt. These iterated variations are complex and risky in both operational and legal terms, but logically they can be considered to be drawn out episodes of perception and maneuver in a large scale hunt for a "high-value target" at the end of an iterated chain of raids.[7]

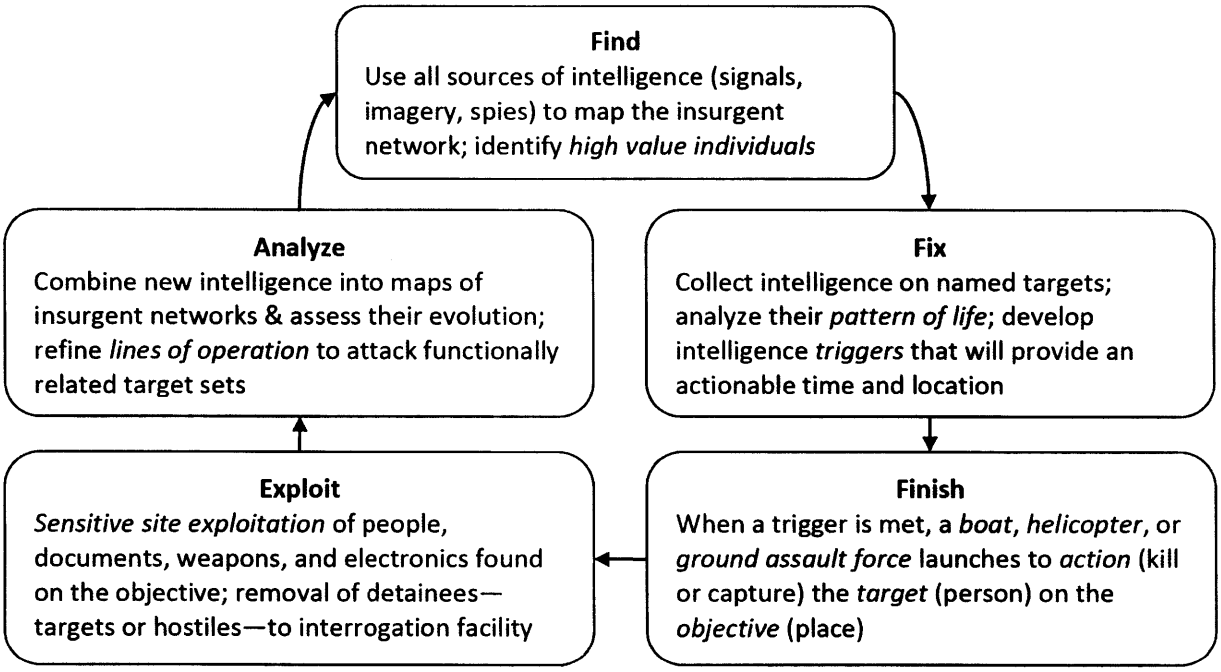


Figure 7-3: U.S. counternetwork targeting methodology ("F3EA") with key jargon in italics

Raids produce more intelligence from detainees and material recovered on the objective, which leads to further raids in a quest to dismantle the enemy network (Figure 7-3).[8] This cyclic methodology, as distinguished from one-off commando exploits or conventional "hearts and minds" counterinsurgency doctrine,[9] is known in U.S. practice variously as "counternetwork operations," "manhunting," or simply "counterterrorism." Figure 7-3 actually describes two

[7] This iterated process is a violent analogue of the ethnographic sampling technique known as "snowball" or "pyramid" interviewing whereby the fieldworker uses referrals from peripheral members of a study group (and referrals from the referrals) to gain access to more centrally-situated and knowledgeable informants.

[8] Michael T. Flynn, Rich Juergens and Thomas L. Cantrell, "Employing ISR: SOF Best Practices," *Joint Forces Quarterly*, no. 50 (2008): 56-61, describe this "F3EA" cycle as implemented by a different SOTF.

[9] U.S. Army, *Field Manual No. 3-24: Counterinsurgency* (Washington, DC: Department of the Army, 2006) actually cautions against relying on special operations raids.

iterations of the general distributed cognition control cycle covered in Chapter 3. *Perception* begins with various signal, imagery, and human intelligence in the "find" phase, which is *integrated* into progressively higher-fidelity maps of the insurgent network and triangulation of particular targets in the "fix" phase, culminating in the *articulation* of a raid in the "finish" phase. The raid produces more intelligence for *perception* in the "exploit" phase, which is fed back into further *integration* in the "analyze" phase in order to trigger the *articulation* of further raids, *ad infinitum*. For simplicity and consistency, I will stick with a single iteration of perception, integration, and articulation in the detailed account below.

7.1.2 The Rise of U.S. Counternetwork Operations

Counternetwork targeting is similar to police countergang stings, as dramatized in the television series *The Wire.*[10] Security forces regularly rediscover this methodology in the course of counterinsurgencies or wherever key information about their foes can only be gleaned through human informants and interrogations.[11] While there is nothing especially new about the concept, the institutions that have grown up to support U.S. counternetwork campaigns in the post-9/11 wars represent something of an innovation at the operational level of war. General David Petraeus, commander of U.S. and coalition forces in Iraq from 2007 to 2008, observes, "There have been breakthroughs in the disciplines of human intelligence, signals intelligence, imagery intelligence [and] measurement intelligence...and each is supported by the proliferation of computer applications, intelligence platforms and growth in various capabilities....But the real breakthrough has been in the fusion of all this...and in the coordination and cooperation of all elements."[12] That is, the innovation has occurred in the elaboration of distributed cognitive systems, as an organizational construct for the collaborative integration of technical surveillance data, far-flung intelligence organizations, and rapid-reaction "finishing forces."

---

[10] The award-winning HBO series dramatizes a police unit's struggles to infiltrate and dismantle Baltimore drug gangs which thrive in an ecology of other social institutions in the city. The series is realistic enough that some U.S. intelligence agencies have used it to educate junior analysts about clandestine networks and their penetration.

[11] Paul Aussaresses, *The Battle of the Casbah: Terrorism and Counterterrorism in Algeria 1955-1957* (New York: Enigma Books, 2002), details a French implementation of counternetwork operations. Aussaresses notoriously describes the use—and efficacy—of torture to gain information from captured Algerian insurgents to drive future operations. The contemporary U.S. implementation substitutes a high-tech surveillance and intelligence analysis architecture for reliance on torture, with some ugly and well-publicized exceptions. For a collection of historical manhunts see George A. Crawford, "Manhunting: Counter-Network Organization for Irregular Warfare," Joint Special Operations University Report 09-7 (2009).

[12] Sean D. Naylor, "Petraeus Sounds Off on Afghanistan: General Says Killing or Capturing Bin Laden Not Enough in Battle Against Al-Qaida," *Army Times* (21 Oct 2008)

The strategic efficacy of the methodology remains an open question. Senior officers like Petraeus make vague pronouncements of success. Journalists have credited the new techniques for severe disruption of militant networks in both Iraq and Afghanistan, yet without any detailed assessment.[13] A few particular success stories, like the 2006 killing of al-Qaeda in Iraq (AQI) leader Zarqawi, have been reported.[14] Yet even the exemplary Zarqawi operation was only a temporary tactical success, for AQI violence continued to climb throughout 2006.[15] As discussed in Chapter 5, AQI was defeated not through the attrition of high-value targets, but instead through the cooperative engagement of tribal militias and American forces. Nevertheless, intelligence-driven counternetwork operations have become integral features of the American way of irregular war.

The relentless violence of the approach stands in stark contrast to "population centric" counterinsurgency in popular and official discourse, as exemplified in the best-selling *Army Field Manual 3-24*. It is certainly possible that "carrot and stick" synergies have been at work: counternetwork attrition may produce "breathing room" for conventional forces to "win hearts and minds," while the large footprint of conventional forces provides intelligence and pressure to flush out the counternetwork quarry.[16] Such interactions and the relative importance of the two approaches—to include their unintended consequences—are quite understudied in the counterinsurgency literature. In practice they coexist as two parallel realities. While the benign

---

[13] Bob Woodward, "Why Did Violence Plummet? It Wasn't Just the Surge," *Washington Post* (8 Sept 2008). Woodward also credits the efficacy of ethnic cleansing prior to the surge, as well as the Anbar Awakening discussed in Chapter 5.

[14] The manhunt for Abu Musab al-Zarqawi is the most publicly detailed case to date of contemporary U.S. counternetwork operations. A series of raids on minor safehouses recovered detainees and computer files, the exploitation of which revealed the identity and habits of Zarqawi's close advisor. This information facilitated tracking the advisor via unmanned aerial surveillance to the meeting location where Zarqawi was eventually killed by an aircraft-delivered precision munition as soon as a team of U.S. commandos on the ground confirmed his presence. For details on the Zarqawi hunt see: Scott Macleod and Bill Powell, "Zarqawi's Last Dinner Party," *Time* (11 June 2006); Mark Bowden, "The Ploy," *The Atlantic Monthly* (May 2007); Matthew Alexander and John Bruning, *How to Break a Terrorist: The U.S. Interrogators Who Used Brains, Not Brutality, to Take Down the Deadliest Man in Iraq* (New York, NY: Free Press, 2008).

[15] Jordan, "When Heads Roll," 720, reports the counterintuitive finding that "Organizations that have not had their leaders removed are more likely to fall apart than those that have undergone a loss of leadership. The marginal utility of decapitation is negative for many groups, particularly for larger, older, religious, and separatist organizations."

[16] Gary Luck and Mike Findlay, "Special Operations and Conventional Force Integration," United States Joint Forces Command, Joint Warfighting Center, Focus Paper no. 5 (2008); US Special Operations Command Pub 3-33, *Conventional Forces and Special Operations Forces Integration and Interoperability Handbook and Checklist* (MacDill Air Force Base, FL: 2006)

"armed social work" or "war among the people" version of counterinsurgency receives more popular attention, the counternetwork juggernaut enjoys generous resourcing, autonomy, and great secrecy. The former fomented a painful learning process for conventional forces,[17] while the latter has been empowered to indulge its preferences.

The SOTF in these pages was but one of many special operations units performing counternetwork operations, some of which were more experienced and better resourced for the mission. Our SOTF additionally had Iraqi security force training and tribal engagement responsibilities, but the counternetwork mission was preeminent in its identity and allocation of information resources. This chapter therefore cannot possibly be an assessment of the methodology in Iraq overall, for some of the problems which I highlight certainly would have been addressed better by other units. Yet this case does provide a window into this emergent but poorly-understood special operations campaign concept, and it also points out some of its potential liabilities. The finding of high levels of information friction in one particular implementation of counternetwork targeting provides a cautionary tale for the uncritical adoption of the policy in U.S. military policy.

This case is based on observations of over 200 direct action missions resulting in the capture of over 300 detainees over the course of a six month deployment.[18] What follows is an unclassified synthesis of the abundant risks to representational validity—and thus of targeting error—that arose. Specific missions, targets, individuals, and intelligence sources and methods cannot be discussed due to classification restrictions, as discussed in Chapter 5. Yet even general patterns of human-computer interactions can raise issues, doubts, and risk factors, even if it is not yet possible to examine their frequency and particular effect on the course of the wars in Iraq and Afghanistan.

7.2 Perceiving Targets

In the perception phase a control system makes physical contact with the battlefield and creates symbolic records that can be moved somewhere else where they can be combined with

---

[17] Colin F. Jackson, "Defeat in Victory: Organizational Learning Dysfunction in Counterinsurgency," Ph.D. Dissertation, Massachusetts Institute of Technology, 2008; Austin G. Long, "First War Syndrome: Military Culture, Professionalization, and Counterinsurgency Doctrine," Ph.D. dissertation, Massachusetts Institute of Technology, 2010.

[18] These numbers appear in unclassified personnel performance evaluations from the deployment.

other records. Perception is never just a passive reflection of objective reality, but rather an active construction of representations to enable practical activity.[19] Operational intelligence highlights features of the world that enable or threaten the operations an organization can perform. The potential *use* of intelligence influences its construction. Most SOTF intelligence was processed under the assumption that it would produce actionable targets. So-called "raw intelligence" was cooked from the get-go.

All sensor data, whether from a human or machine, undergoes processing between the instant of physical transduction and transmission to an analyst who can work with it. While the technical means of collection are closely guarded secrets, the dissemination of raw intelligence becomes a matter of routine within a military enterprise. Standardized reporting channels and formats reliably and repeatedly deliver records of contact with the battlefield. The process is something of a black box for most personnel. Like any black box, however, the stability of the output hides a lot of assumptions built into the architecture. Each step can discard provenance data or introduce spurious information. For instance, say that a sensor provides a set of geocoordinates of something in its field of view at a particular time, but for some reason the machine is unable to resolve the coordinates and sends, by design default, the most recent coordinates in memory. When many handheld GPS units are first turned on and awaiting a satellite fix, they display their last known location, which could be miles away if the unit was moved while it was turned off. Likewise, if only the coordinates and time were included in the raw intelligence report from our notional sensor, then an analyst might assume the entity remained fixed when in fact it had moved. This simplistic problem might be easily corrected by also including a metadata field indicating whether the coordinates were default or not—*if* the sensor device exposed that data and *if* it was accessible to transmission. Simplifying assumptions within any link of the representational chain may introduce errors because any black box assumption is "leaky" in some circumstances.

Intelligence personnel with experience in different collection disciplines (signals, imagery, human espionage, *etc.*) over a long career usually cultivate a feel for pitfalls in specific lines of collection and means of representation. Given the SOTF's last-minute personnel

[19] Richard Rorty, *Philosophy and the Mirror of Nature* (Princeton, NJ: Princeton University Press, 1979)

augmentation and underinvestment in "tech" training (as described in Chapter 5), its level of experience in the craft of intelligence was uneven. Thus many black boxes were not opened.

7.2.1 Signals and Noise

Contemporary signals intelligence (SIGINT) runs on a sprawling organizational and highly technical architecture.[20] In an earlier era cryptographers like the mathematicians at Bletchley Park focused on making and breaking codes, but SOTF "cryppies" were situated far downstream of encoding and collection, so they acted as gatekeepers for machines that delivered SIGINT from national, theater, or organic sources.[21] Behind formidable classification and cultural barriers, this priesthood decided what information would be made available to the rest of the SOTF. Technicians stripped out data that identified a particular hard-to-replace collection capability in order to create the plausible illusion that it might have come from a less sensitive source (*i.e.*, maybe a conversation was overheard by a human spy rather than electronically intercepted). Such "sanitization" intentionally obscured the provenance of data used outside of the sensitive compartmented information facility (SCIF).

Like the network administrators who kept computer networks running with little interest in content, cryptologists had limited understanding of how or when SIGINT might be combined with other intelligence for operational use. "All-source" analysts had to overcome epistemic and security barriers to the technical supply of intelligence, which both lowered the probability of articulating black-box assumptions and increased the chance that useful data might not be brought to bear. An Iraqi who appeared to be a key node in a network of insurgent communications could end up having some legitimate alibi which might only be gleaned through consulting other types of non-SIGINT intelligence: maybe he was just a local money-lender or

---

[20] On SIGINT technologies and organizations see: David Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet, Rev. Ed.* (New York, NY: Scribner, 1996); David Alvarez, ed., *Allied and Axis Signals Intelligence in World War II* (London: Frank Cass, 1999); Robert J. Hanyok, *Spartans in Darkness: American SIGINT and the Indochina War, 1945-1975* (Ft. Meade, MD: Center for Cryptologic History, 2001); James Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency from the Cold War Through the Dawn of a New Century* (New York, NY: Doubleday, 2001)

[21] This is an instance of "deskilling" whereby operators who once did work become supervisors of machines which do the work. See David F. Noble, *Forces of Production: A Social History of Industrial Automation* (New York, NY: Knopf, 1984); Shoshana Zuboff, *In the Age of the Smart Machine: The Future of Work and Power* (New York, NY: Basic Books, 1988); Duncan Gallie, "Patterns of Skill Change: Upskilling, Deskilling or Polarization?" *Work, Employment & Society* vol. 5, no. 3 (1991): 319-351

delivery boy who was often on the phone. Conversely, cryptologists might not bring in potentially valuable SIGINT if unaware of how some all-source analysis was developing.

Apart from its analytical role, SIGINT data also served to reinforce social boundaries. Some staff personnel made a fetish of SIGINT by making regular pilgrimages into the SCIF if cleared to hear the latest news. Some personnel conflated the value of signals intercepts with the height of institutional barriers protecting access to them.

7.2.2 Manipulating People

Rather than arms length technical collection, the first step in the human intelligence (HUMINT) cascade of inscription often involves indigenous sources who inform on and betray their comrades.[22] The paradoxical task of espionage is to ensure that agents can be trusted enough to lie. The checks and balances which enforce reliable relations in a bureaucracy work at cross purposes with the tradecraft which enables agents to survive counterintelligence attention.[23] There was thus always a risk that Iraqi agents could report on "terrorists" to liquidate personal grudges, fabricate stories to make money or enhance their status, play different U.S. HUMINT organizations off one another, or infiltrate as double agents to lure American soldiers into an ambush.[24] HUMINT collectors vet agents by cross-checking their reporting and asking them to undertake nontrivial observable tasks to signal their reliability, but there are ultimately no perfectly reliable means for establishing *bona fides*. Espionage injects instability into representational cascades at their source.[25]

---

[22] I'm focusing primarily on the use of clandestine spies. HUMINT is a broad category that also includes interrogations of captured personnel, tactical questioning and observations by soldiers on patrol, debriefings of U.S. personnel, etc. Interrogation and document exploitation will be discussed in the section on articulation.

[23] Derek Jones, "Understanding the Form, Function, and Logic of Clandestine Cellular Networks: The First Step in Effective Counternetwork Operations," School of Advanced Military Studies, United States Army Command and General Staff College (Fort Leavenworth, Kansas: 2009), provides a good summary of clandestine communication methods in insurgency and espionage: cellular organization, cut-outs, dead drops, couriers, codes, safe houses, surveillance detection, reconstitution plans, *etc.* Diego Gambetta, *Codes of the Underworld: How Criminals Communicate* (Princeton, NJ: Princeton University Press, 2009), examines the problems spies and criminals face in communicating their identity and capabilities to co-conspirators while hiding it from rivals and law enforcement.

[24] A suicide bomber who killed seven CIA officers in December 2009 was an al-Qaeda double agent: Richard A. Oppel, Jr., Mark Mazzetti and Souad Mekhennet, "Attacker in Afghanistan Was a Double Agent," *New York Times* (4 January 2010)

[25] On contemporary HUMINT see Frederick Porter Hitz, *The Great Game: Myth & Reality of Espionage* (New York: Vintage, 2005); I. E Prikhodko, *Characteristics of Agent Communications and of Agent Handling in the United States of America* (San Francisco, CA: Interservice Publishing, 1981). On military HUMINT in Iraq: Charles W. Innocenti, Ted L. Martens and Daniel E. Soller, "Direct Support HUMINT in Operation Iraqi Freedom," *Military Review* (May-

7.2.2.1 Bureaucratic Tradecraft

Responsibility for SOTF HUMINT was spread across SEAL Team intelligence personnel, Office of Naval Intelligence augmentation, and a nascent organic component.[26] Intra-organizational turbulence and steep learning curves exacerbated HUMINT's inherent challenges. Furthermore, the same skills that were useful for manipulating Iraqi sources were also useful for manipulating colleagues. HUMINT collectors—and support personnel living vicariously through them—leveraged their enigmatic autonomy to enhance influence and prestige. Relaxed grooming standards, civilian clothes, segregated work spaces, and IT systems disconnected from common networks ostensibly facilitated covert collection and source protection, but they also inhibited performance audits and asserted an exceptional status.

The SOTF's HUMINT subculture, to a far greater degree than the cryppies with their geeky "tech" stigma, put up barriers to mutual understanding and affected a cagey air of elitism. The fetishized protection of HUMINT tradecraft, the essence of which is as old as espionage and well-described in open sources, not only created social barriers within the SOTF but also degraded analysts' understanding of the very means their insurgent targets used to communicate with one another.

7.2.2.2 Reporting Bias

The search for HUMINT sources and the lines of questioning pursued during meetings with sources were developed primarily to elicit names and locations of kill/capture targets. Reporting focused narrowly on suspected insurgent operatives rather than local political, economic, or tribal dynamics which might have enabled indirect modes of neutralizing insurgents and enhanced understanding of local atmospherics. The irony is that local politics and motivations for fighting (or defecting) were often discussed in the course of vetting and establishing rapport with Iraqi sources, which was just the sort of data that could be of great value to analysts looking to understand the broader social context of the war. Yet it remained segregated in source-management computer systems or was never recorded at all because

---

June 2009): 48-56; Ralph O. Baker, "HUMINT-Centric Operations: Developing Actionable Intelligence in the Urban Counterinsurgency Environment," Military Review (March-April 2007): 12-21; Department of the Army, *Field Manual 2-22.3, Human Intelligence Collector Operations* (Washington, DC: 2006)

[26] For a description of HUMINT with NSW Task Unit Ramadi, see Dick Couch, *The Sheriff of Ramadi: Navy SEALs and the Winning of Anbar* (Annapolis, MD: Naval Institute Press, 2008), 40-41, 219-222.

collectors didn't believe that outsiders needed to know. Moreover, every detail reported required additional time spent typing, so much tacit information was never articulated.

Intelligence analysts read only finished reports that sanitized source identity and summarized a meeting. Report quality depended on the HUMINT collector's experience, writing skills, and enthusiasm for detail; these three qualities were often in short supply in the SOTF. Descriptions might be vague (*e.g.*, the phrase "a man with a mustache in a *dishdasha*" describes most Iraqi men) or uncritically reflect source opinions ("that man is a terrorist"). Collectors were unlikely to advertise the low quality of any agents they kept on the books to boost performance metrics. HUMINT collectors who spoke directly to target-hungry operators might not even write reports, further degrading all-source fusion and auditing efforts.

In an example of expedient adaptation, it was common practice in Iraq to produce "draft" intelligence information reports (DIIRs) in Microsoft *Word* and disseminate them via email rather than through the cumbersome bureaucracy for filing official IIRs. This hack also became a source of friction as the DIIR serial number was changed to a new IIR serial number once the report was finally edited and re-released in official IIR reporting databases. The resultant ambiguity of source references complicated intelligence validation, but the improved ease of drafting and disseminating DIIRs prior to IIRs made up for it.

7.2.2.3 Uncertainty in the Direction of Control

While HUMINT potentially offers close contact with the population and unique atmospheric and political information, it was hardly an unbiased instrument. Collectors' targeting ambitions were reinforced by Iraqi sources eager to please and get paid for their efforts, or more ominously, to exercise their own targeting ambitions. American HUMINT collection provided one avenue for Anbari tribes to co-opt American military muscle to settle local tribal and criminal scores that they were unable to address themselves. The fortunate alignment of American and tribal interests against al Qaida forestalled difficult questions of who was running whom in HUMINT relationships.[27] SOTF collectors bristled indignantly at the suggestion that their sources might be out of their control ("my sources don't lie!"), and so such questions—especially from second class "techs"—were discouraged. The search for targets *per se* and the

[27] The degree to which American force was "under control" of the tribal source network, like the micro-causes of the Anbari turn in general, remains an open historical question.

willingness of sources to provide them created a filter on the type of information which entered the SOTF in the first place.

7.2.3 The Blinking Eye

Intelligence, surveillance, and reconnaissance (ISR) refers to the entire constellation of manned and unmanned air, space, sea, and ground based sensors supporting military operations. In practice at the SOTF, "ISR" referred mainly to unmanned aerial vehicles (UAVs) with real-time full-motion video in the visual and infrared spectrums for day or night coverage, although UAVs also carried other types of sensor payloads. The overall number of ISR platforms in Iraq increased tenfold between 2003 and 2008, expanding from two to over a dozen different types of aerial full motion video, with a threefold increase in intelligence personnel at the battalion level to support it.[28] The Orwellian vocabulary of ISR—"unblinking eye" and "persistent stare"—conveys the ambition of expanding imagery and signals collection over larger areas of terrain at greater levels of fidelity for more of the time. Small units can thus control long-dwell, non-invasive, real-time surveillance video, lessening the need to risk and support scouting patrols on the ground. Higher headquarters can also keep tabs on and intervene in operations in real-time. Inevitable gaps in coverage drive demand for more collection platforms and more management to coordinate them all. The challenge for all echelons is to recover the context of disembodied video.

7.2.3.1 Remote Control

Most intellectual attention to UAVs has focused on the "unmanned" part, both in terms of the experiential and legal novelty of fighting by remote control and the cultural displacement of pilots within aviation organizations.[29] The UAV operator can be located on the other side of the

---

[28] Raymond T. Odierno, Nichoel E. Brooks and Francesco P. Mastracchio, "ISR Evolution in the Iraqi Theater," *Joint Forces Quarterly*, no. 50 (2008): 51-55. The article also shows how conventional forces are also conducting the type of ISR-driven counter-network operations pioneered by SOF, which illustrates (1) that SOF often serve as early adopters of technology and tactics that later diffuse to conventional forces, and (2) the convergence between conventional forces and "hyperconventional" SOF who do the same missions, just faster and more capably.

[29] Unmanned aircraft introduce painful questions of identity for organizations like the Air Force or naval aviation built around manned aircraft; Thomas P. Ehrhard, "Unmanned Aerial Vehicles: A Comparative Study of Weapon System Innovation," Ph.D. Dissertation, Johns Hopkins University School of Advanced International Studies (2000). For an introduction to the moral and organizational dilemmas of unmanned vehicles, see: P. W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York, NY: Penguin Press, 2009). On the legal issues in remote control killing in counter-terrorism operations, see Kenneth Anderson, "Targeted Killing in U.S. Counterterrorism Strategy and Law," Working Paper in Counterterrorism and American Statutory Law, Brookings Institution, Georgetown University Law Center, Hoover Institution (2009).

planet, connected via satellite from Nevada in the case of the MQ-1 Predator drone. Sensor video was broadcast over the Secret internet (SIPRNET) so that anyone in the theater could subscribe to the feed to watch collection vicariously. To direct the sensor to follow a particular vehicle or individual, or to zoom in on a particular house, SOTF Task Unit personnel communicated with UAV operators using a standard commercial chat room client over SIPRNET. Sometimes too many chat room lurkers inadvertently blocked users who were actually guiding and monitoring the operation from reconnecting after a dropped circuit.

SOTF headquarters participation in the ISR hunt was limited to scheduling coverage from UAVs controlled by the SOTF's higher headquarters. Because target development actually took place at the Task Unit, the SOTF ISR manager just scheduled UAV coverage, much as the air operations officer scheduled aircraft for transporting people and gear. This contributed to a fragmentation of the ISR fusion effort, in that the Task Units might not understand the capabilities and limitations of specific platforms or the range of collection options, while the SOTF did not understand how exactly the Task Units were using ISR.[30]

7.2.3.2 Video Data Management

Less attention has been paid to downstream data-processing than to the teleoperation of drones. By one estimate, the amount of intelligence data flowing back from automated surveillance technologies has increased by 1,600% over the last decade.[31] UAVs collected over 200,000 hours of video in 2007 over both Iraq and Afghanistan, but there was no automated way to find and catalog interesting results.[32] A human observer at a Task Unit had to watch long stretches of video where nothing out of the ordinary occurred as Iraqis went about their daily life. Personnel had to concentrate to stay oriented through the "soda straw" of the sensor. Remarkably, they did not know how to use a simple tool to plot the sensor field of view over a

---

[30] Collection management is a classic intelligence function connecting prioritized analyst requirements with all types of collection systems across technical disciplines. In the broader intelligence community, collection management is a formalized bureaucratic process for allocating national assets, which not only helps to manage limited resources but also to sanitize the intelligence to protect sources and methods. In another instance of underinvestment in information expertise, the SOTF's *ad hoc* method for meeting this key function was to get an ISR manager from the Office of Naval Intelligence, a service level agency with no particular competence with tactical ISR.

[31] Thom Shanker and Matt Richtel, "In New Military, Data Overload Can Be Deadly," *New York Times* (16 January 2011)

[32] Christopher Drew, "Military is Awash in Data from Drones," *New York Times* (10 January 2010). The Air Force is working on incorporating video tagging software used by news and sports organizations to facilitate archiving and search of this massive take, but this capability was not available in 2007-8.

FalconView map display which had been developed by Air Force users *five years* before; this is another incidence of uneven IT literacy at the SOTF as well as the persistent "stickiness" of situated knowledge.[33] ISR analysts might snip out bits of video and attach it to an email with text reading, "Check out around 1:32 where the cars stop at the canal." Without both the email and the attachment, there was no way to know that there was in fact video of something interesting. Furthermore, because watching ISR was a tedious task, it was often delegated to very junior personnel who might not be steeped in target development or familiar with cross-cues from other intelligence sources, which lowered the chance that interesting things would be noted in the first place.

Personnel stored ISR video snippets in a share drive folder for whatever target the Task Unit was tracking when they requested ISR. This historical video could conceivably be useful for other target development.[34] Yet without a geographic database of tagged ISR coverage, or a fortuitous conversation with the analyst who watched the video, there would be no way to search for these clips. The traces of ISR collection were deposited in target-specific cubby holes on the share drive, and whatever assumptions went into choosing them were lost. Often the only real reference to ISR clips was in the head of the analyst who did the observing and cutting. There was no common catalog, and hence little corporate memory of ISR collection. These particular search and cataloging problems, if set against a stable frame of reference of space and time, would seem solvable enough through automation. Indeed, ISR is flush with opportunities for expanding control by improving standardization and enterprise integration, but only *if* participants agree on video tagging categories and procedures. At the SOTF those categories were embodied in folder structure and comments on emails with attached comments, and they varied significantly across targets, analysts, and Task Units.

---

[33] It was possible to use geocoordinates from the UAV, steamed over SIPRNET, to drive a live feed on *FalconView*, which could plot a box for the sensor field of view on top of a map or image layer, thus providing much broader situational awareness for the sensor operator. This capability was pioneered in 2001-2003 by Air Force officers supporting multiple Predator missions in Afghanistan, and thus was well known within the ISR community; Paul Hastert, "Spiral Development in Wartime," *PowerPoint* presentation, provided to author (2005).

[34] Past coverage could, ideally, be used to develop a baseline against which to compare new coverage in order to establish that the analyst's "something interesting" was a genuine anomaly, rather than a selection bias that made a target appear more "nefarious" than it was. Alternatively, "something interesting" might never be noted even though it would have appeared suspicious against a baseline (*i.e.*, Sherlock Holmes' "dogs that don't bark").

I will return to the use of ISR to monitor the execution of raids—colloquially known as "kill TV"—in the discussion of the articulation phase of control.

7.2.3.3 Incremental Improvement of Targeting Support

ISR offers seductive opportunities to capitalize on network-centric concepts, but it's easy to underestimate the management overhead of coordinating this complex constellation of humans and machines. Fortunately, the problems of detecting an insurgent emplacing an IED, or of following a target's car to a safehouse, or of providing overwatch for a patrol, are all fairly proscribed and tractable problems. The basic concept of "persistent surveillance" is straightforward enough, and the implementation just complicated enough, that ISR can occupy a tremendous amount of effort in incremental improvement. ISR is well suited to following targets and overwatching finishing forces. Thus contractors flock to trade shows in droves to improve ISR mousetraps, and professional journals brim with sanguine stories of improving the time-latency, area-coverage, responsiveness, collaboration, and low-echelon availability of ISR. Improvements in these narrowly proscribed problems can be considered RMA success stories.

However, there are opportunity costs. The attention to improvement of the means of target perception is also attention not spent in considering the ends of targeting, or alternative ways of accessing and disseminating information about the population, to say nothing of the ethics of the Orwellian "unblinking eye" in the nominal democracy the counterinsurgent hopes to reconstruct. ISR is a solvable engineering problem that abstracts away the human allies and adversaries which actually drive the war. Might it be cheaper and easier to interact with locals on the ground in order to find someone, to understand who he is, and why something is happening? Or to negotiate with indigenous partners for solutions that obviate the complicated ISR-driven hunting drill? What right to privacy should citizens in the "protected population" hope to enjoy? These questions are outside of the prevue of RMA discourse on ISR.

7.2.4 Lost in Translation

Most alternatives to ISR require actually talking to the locals. Five years into the war in Iraq, most U.S. personnel had little familiarity with the Arabic language, let alone the Iraqi dialect. Uniformed linguists were few, concentrated mainly in SIGINT with rudimentary proficiency in Iraqi Arabic, and thus heavy reliance on Iraqi interpreters across the spectrum of operations was unavoidable. Militaries which conduct "war amongst the people," ironically,

tend to chronically under-invest in the ability to talk to those people. Training in tactical proficiency and technical fixes offer a shorter return on investment, especially for an active duty and reservist population constantly rotating through different jobs. Language barriers created friction across the board for the SOTF, but they were arguably more problematic for indirect action missions because they depended so much on local communication and because more interpreters were dedicated to direct action support.

7.2.4.1 Terps

HUMINT and SIGINT collection, interrogation and document exploitation, training and operating with security force partners, meetings with tribal elite, and logistics coordination all depended on Iraqi interpreters ("terps" in military idiom). Most SOTF interpreters were Iraqi-born American citizens who held Secret-level clearances. While this controlled adequately for loyalty,[35] interpreters might still have their own agendas for adventure or revenge (some had fled the abuses of the Baath regime). Differences in their dialect and religious sect could sometimes offend local Iraqis (Anbar was largely Sunni whereas many refugees from Baathist Iraq were Shia or Christian), who tended to see interpreters as traitors or collaborationists. In HUMINT meetings conducted through an interpreter, Anglophone collectors had difficulty developing rapport and reading nuance in speech and culturally-specific body language, which is essential to establishing control over an informant. Some collectors even allowed their interpreter, untrained in tradecraft, to run the meeting.[36] Interpreters were the gatekeepers to linguistic access to the population, and thus another source of equivocation at the source of cascades of inscription.

7.2.4.2 Transliteration

Local names and phrases were transliterated into English for intelligence and operational products. While there were a number of transliteration guides floating around, adherence to standards was irregular, which complicated database searches and information management. Personnel complained, "There are so many ways to spell 'Mohammad' ['Muhammad,' 'Mohamed,' *etc.*]; we need to standardize!" The irony is that there is just one way to spell it in

---

[35] The ubiquitous presence of 'terps in counterinsurgency makes them a significant counterintelligence risk

[36] Most HUMINT professionals insist that the interpreter should carefully translate everything the informant says, like a UN translator, so that the social interaction is between the collector and the informant, with the interpreter kept off to the side. In practice, many collectors would let their 'terp simply gloss the informant's comments and provide opinions. Thus large amounts of speech from a detainee might be summarized by something like, "He says he doesn't know anything, but he's a lying piece of crap."

Arabic (محمد). The Arabic version was hardly ever included in intelligence reporting or databases, so analysts had little incentive to bother to learn the alphabet, even after years of working Iraqi problems. Iraqi names furthermore include references to multiple family generations and tribal affiliation, but transliterations usually only included three names, often shortened to three-character initials, and they might not necessarily be the same three names across reports. American maps often did not include Iraqi names for local streets and places, but instead featured overlays with American nicknames or numbers; this improved coordination with other Americans but not with Iraqis.

Intelligence organizations sought to address these problems not through increasing Arabic language competency among analysts, but through automated translation systems and sophisticated pattern-matching algorithms to link transliterations and naming variants. The community sought to offload linguistic fluency onto the distributed cognitive system rather than its human members, creating a perverse situation of increasing returns to illiteracy. The self-inflicted confusion over transliteration standards helped to insulate a stubbornly English-speaking military from its Arabic environment.

To sum up the SOTF's perception phase of control, cascades of inscription were long and complicated chains of transformation. Especially in the case of signals and imagery collection, there was a sophisticated technical and institutional apparatus to channel the cascades, which meant that operations inside of nested "black boxes" were not readily auditable. In all forms of collection, there were plenty of opportunities for human interpretation and selection, or suppression, of some features over others to propagate into further representations. All of the degrees of freedom in transforming representations and in cut-and-pasting data created high potential for equivocation and loss of provenance. Yet above the general level of noise, the built in bias for selecting information which conformed to a targeting view of the world was notable. Channels for targeting information were more robust and actively stabilized by humans and machines, so much so that some of the equivocation was masked in the construction of targets.

7.3 Integrating Multisource Data

In the integration phase of control, the information system gathers records of perception into "centers of calculation" where they can be combined with each other and with information

in memory. *Fusion* is the intelligence term of art for combining multiple intelligence reports from multiple sources to discern operationally-meaningful patterns. Fused intelligence enables people to make sense of the location, timing, and relationships between entities on the battlefield so they can determine valid targets and develop strategies to intersect with them.

Chapter 6 described how the proliferation of modern IT fosters the emergence of multiple centers of calculation on different computers or even in different applications on the same workstation. Digital information moves easily over internetworks and combines via cut-and-paste, so any of the applications reviewed in Chapter 6 (*PowerPoint*, email, geospatial mapping, *etc.*) could serve as sites for fusion. The SOTF's cascades of perception and articulation involved many intermediate centers sited in these applications, with no one single apex (in contrast to the map table in Fighter Command's Operations Room in the Battle of Britain in the next chapter). The important apices in the SOTF's cascades of inscription were not as much physical places as genres of digital representation which might be viewed on various computer monitor or displayed on a projector.

SOTF briefings to visitors regularly evoked the word "fusion" to describe ops-intel cooperation to overcome information boundaries, but it really just underlined their persistence. There was not any specific methodology for constructing valid representations in a center of calculation. The SOTF did not and could not have one master fusion system because personnel combined information in a number of fragmentary and overlapping representations. One person's fused intelligence product could be another's input material for a new project. It could be difficult to tell with some products how much upstream incorporation of new data or interpretation there had been, or if instead the same snippet of text had simply been cut-and-pasted, reformatted and repackaged multiple times.

7.3.1 Social Networks

Chapter 6 deferred discussion of one major genre of digital representation at the SOTF because of its role in the counternetwork mission. Social network diagrams map the semantic relationships between entities and events. Photos on bulletin boards and criminal organization charts have long been staples of police countergang investigations and military counterinsurgencies. Now that digital IT enables the representation of networks with thousands of links and nodes, intelligence organizations invest heavily in the construction of large social

network data sets, and IT-intensive social network analysis has become a basic tool in the counterinsurgency intelligence toolbox.[37]

As a rhetorical staple of the information age, furthermore, many people have used network concepts to describe everything from gene transcription to whole economies.[38] Unsurprisingly, RMA militaries thus describe themselves and their adversaries as "network centric" or "network enabled."[39] Social network analysis occupies a prominent place in this rhetorically-charged milieu: robust IT networks of networked organizations should enable social network analysis to defeat a self-organizing network of terror. However, irregular warfare is more than just a set of links and nodes (one *Wired* article observes that "in Iraq, the critical networks are social—not electronic"[40]), and furthermore, the working practice of constructing digital social network diagrams can obscure as much as it reveals. Panoptic fantasies of social network modelers are defeated by collective action problems in the construction of models. This section highlights the friction which emerges in the social life of social network analysis.

7.3.1.1 Ambitions to Map the Entire Network

The counternetwork fusion ideal is a social network model that completely and accurately reflects the relationships between all terrorist operatives and facilitators. This model would be constantly updated with new intelligence from an interagency dragnet. The vast database of links and nodes would submit to analysis with mathematical graph theory to measure things like "betweenness centrality" or "structural cohesion" to identify which "critical nodes" should be removed to dismantle the network. Computers would generate dramatic visualizations (Figure

---

[37] Department of the Army, "Appendix B: Social Network Analysis and Other Analytic Tools" in *FM 3-24,Counterinsurgency* (Washington DC: 2006); Carlo Morselli, *Inside Criminal Networks* (New York, NY: Springer, 2009)

[38] Albert-Laszlo Barabasi and Eric Bonabeau, "Scale Free Networks," *Scientific American* (May 2003); Duncan J. Watts, "The 'New' Science of Networks," *Annual Review of Sociology* vol. 30 (2004): 243-270; Emilie M. Hafner-Burton, Miles Kahler and Alexander H. Montgomery, "Network Analysis for International Relations," *International Organization* vol. 63, no. 3 (2009): 559-592; David Knoke and Song Yang, *Social Network Analysis, 2nd Ed.* (Thousand Oaks, CA: Sage Publications, 2008).

[39] Marc Sageman, *Understanding Terror Networks* (Philadelphia, PA: University of Pennsylvania Press, 2004); John Arquilla and David F. Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001)

[40] Noah Shachtman, "How Technology Almost Lost the War," *Wired* (27 November 2007). Jones, "Form, Function, and Logic," discusses the discrepancy between the structure of clandestine networks and the "small world" network concepts that grounds most social-network analysis of insurgency and terrorism.

7-4) so that officers could pick targets as in a schoolhouse wargame.[41] The design of network analysis and visualization software is a major cottage industry in the counterterrorism world, built on the assumption that reasonably clean and complete terrorism data will be available for systems.

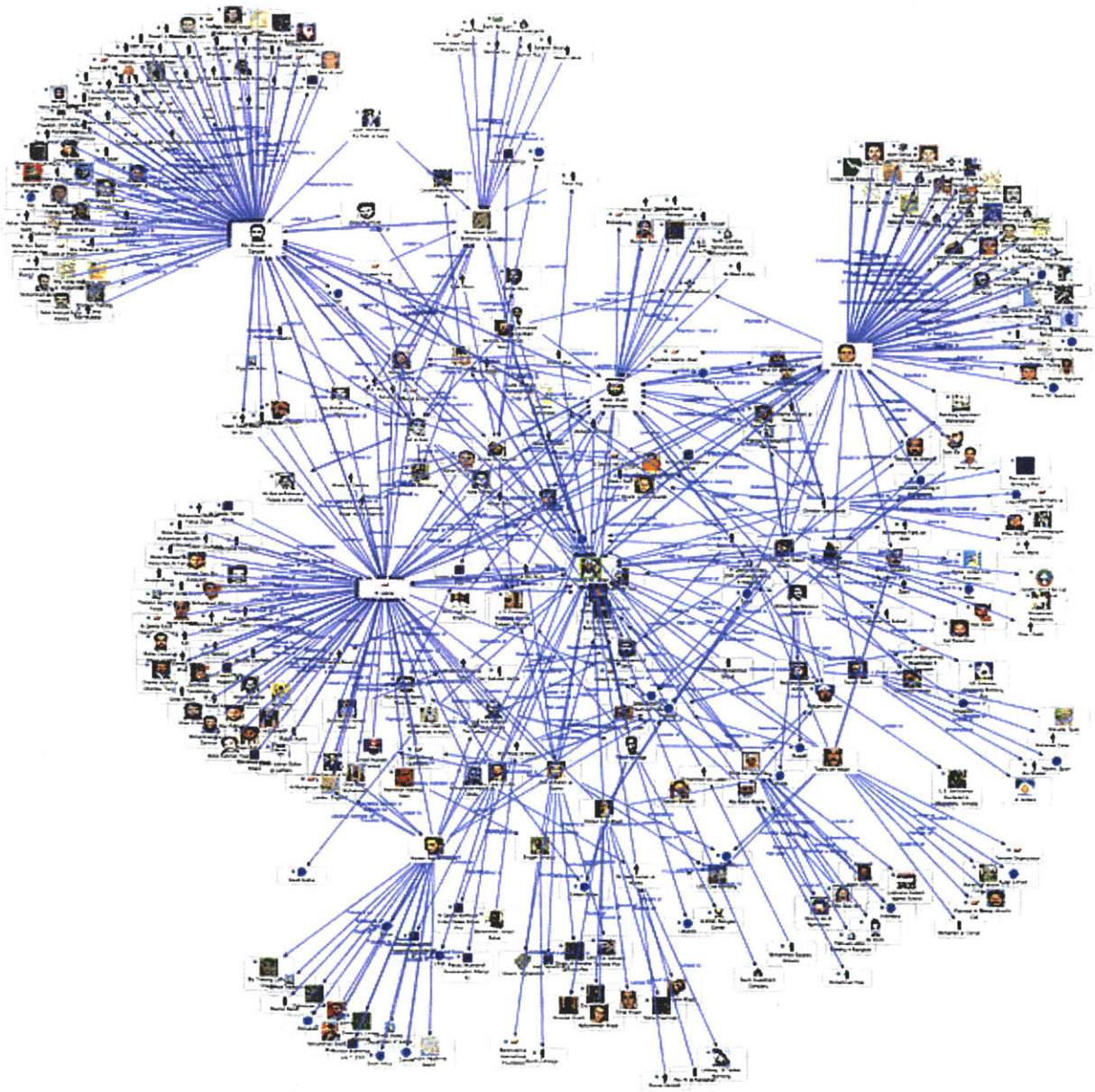


Figure 7-4: Social network diagram of a terrorist organization with a computer-generated layout

[41] Figure 7-4 from promotional material from FMS Advanced Systems Group (an outfit capitalized by the CIA-affiliated venture capital firm In-Q-Tel), http://www.fmsasg.com/SocialNetworkAnalysis/ [accessed 8 December 2009].

The basic metaphor of *nodes* and *edges* (*links*) from graph theory is versatile enough to represent the various economic, bureaucratic, or personal relationships which make up an illicit network. The methodology is invaluable for showing visually how the adversary is a clandestine *organization* rather than an amorphous mass of fighters; for representing the personal relationships and micro-level transactions which embody the organization; and for keeping track of a large number of people, places, events, and relationships in forensic analysis of past attacks and projections of future activity.

Yet this great flexibility is also a liability. In practice in Iraq, the methodological problems reviewed below undermined the integrity of social network analysis. Analysts defined links and nodes incommensurably across different applications, so their partial diagrams (or "subgraphs") were ontologically incompatible. Analysts encoded information in the visual layout of their diagrams, so the data was inaccessible to graph-theoretical algorithms operating only on links and nodes. The real insurgent networks evolved at the same time that analysts built their time- and labor-intensive diagrams. These diagrams did, nevertheless, have local utility. They served a heuristic role to help small groups of analysts keep track of reporting on a circumscribed problem. They also served a more rhetorical role to help sell particular targets.

7.3.1.2 Ontological Design Decisions

The problem of incompatible definitions of links and nodes is similar to the problem of idiosyncratic map overlays discussed in Chapter 6, but without any common base map layer or mature craft standards as with cartography. Analysts enjoyed substantial interpretive flexibility to decide what to include in diagrams as they read reports. Table 6-1 lists some of the mundane design decisions that analysts had to make, each of them with consequences for data-entry workload and the results of graph-theoretic analysis. For example, if the analyst decided to include a "located in" relationship between insurgents and the city "Fallujah," then Fallujah would, absurdly, be the critical node in the social network. Analysts (like database engineers) might argue about which typologies were best, but inevitably they encountered situations while reading new reports which did not fit the "correct" ontology they had agreed upon. How should one diagram a report about a schoolteacher sexually blackmailing his brother to smuggle IED parts strapped to the bellies of his flock of sheep?

Table 7-1: Examples of social network diagram design decisions

Design decisions about social network diagrams and confusion over provenance metadata
• Are nodes only people, or also places, weapons, houses, animals, and bank accounts?
• Do we include just "red" insurgent data, or also "green" civilians and "blue" friendlies?
• Should relationships be stable like kinship or partnership, transient like "bought some phones from," or accidents of geography like "lives next to"?
• Should there be a node for every city, neighborhood, and house? Should we include multiple "located within," "born in," and "visited" relationships between people and locations, or should those just be properties of the people nodes?
• Should there be multiple relationships between two nodes for multiple visits to the same location, or separate "event" nodes for each visit linked to all parties?
• Should the imam of a Mosque be named "al-X Mosque Imam" or should the node have his personal name with a link to the mosque called "imam of"?
• Should I cite sources for this information, and if so do I need to cite them for every link and node? Should I attach sources to the node or to the whole network?
• Should I take a few hours to diagram everything in this report (and all the others that came in today), or just what seems relevant to the problem I am thinking about right now?

Many analysts, unconstrained by software or standards, simply used a default label called "associated" for relationship links. If the analyst who built the diagram wasn't available or couldn't remember the original reporting, then it would be difficult to discern whether two "associated" nodes meant villainous collusion, romantic tryst, or just some guy who delivered eggs occasionally. Different answers to questions like those in Table 6-1—often made tacitly in the course of building diagrams—led to incommensurable diagrams that could not be aggregated into larger computational models without prohibitive amounts of clutter.

When were diagrams most likely to be commensurable and scalable? When durable real-world infrastructure—like electrical power grids, bank transactions, or telephone networks—supported the homogeneous typing of nodes and edges, then network diagrams could map onto the real world in a more standardized way: all nodes are phone numbers, and all edges are calls between them; all nodes are electrical substations, and all edges are powerlines; *etc.* Not coincidentally, engineers design such infrastructure to include mass-produced links and nodes with regularly repeated interactions across them. That is, durable network ontology on the battlefield (a component of the external stability variable defined in Chapter 4) enabled more

reliable network diagrams. Mathematical analysis could then identify relevant topological features in the model that reliably mapped back onto real-world structure.

By contrast, the ontological heterogeneity of normal social systems, let alone clandestine organizations, frustrated the stabilization of node and link definitions for comprehensive, all-inclusive diagrams. Even seemingly stable relationships like kinship were tricky because of variable cultural interpretations and practices. Network ontology could be enforced by work-center policy or agreed on by consensus, but analysts would inevitably work around it or use the mandated categories in surprising ways as they came across new reporting.

7.3.1.3 Information in Visual Layouts

The technical tools used to build social network diagrams had affordances for individual users which further hindered the aggregation of social networks into models amenable to mathematical analysis. Most analysts used a software package called *Analyst's Notebook* as a large graphical canvas to arrange linked entities, more-or-less like a huge *PowerPoint* slide with sticky links between objects. They did not usually exploit the powerful graph-theoretical analytical functionality in the application; moreover, as they added data which depended on a particular spatial layout, they *could not* use that functionality without losing data.

As with color-coded *Excel* spreadsheets, the visual layout of entities on the diagrams encoded important information. Compare the human-produced *Analyst's Notebook* layout in Figure 7-5 below to the computer-generated "hairball" in Figure 7-4 above. Figure 7-4 only has people with linked associations between them, laid out by an algorithm based on the graph-theoretical structure of the network. Figure 7-5 has a more complicated ontology of people (living and dead), places, organization, equipment, and activity. Figure 7-5 also has an informative visual layout with text labels and bounding rectangles which implicitly define organizational associations. The enclosure of icons representing people in a rectangle representing an organization implies a *semantic* relationship between all these people, but because there are no explicit links drawn between the people, a computer could not *syntactically* operate on the associations.[42]

[42] Standard graph algorithms take a set of links and a set of nodes as inputs. Obviously a computer could be programmed to link all the entities inside of a bounding rectangle, but that involves a lot of additional design assumptions about how exactly to interpret implicit bounded links and explicit links to both bounded entities and

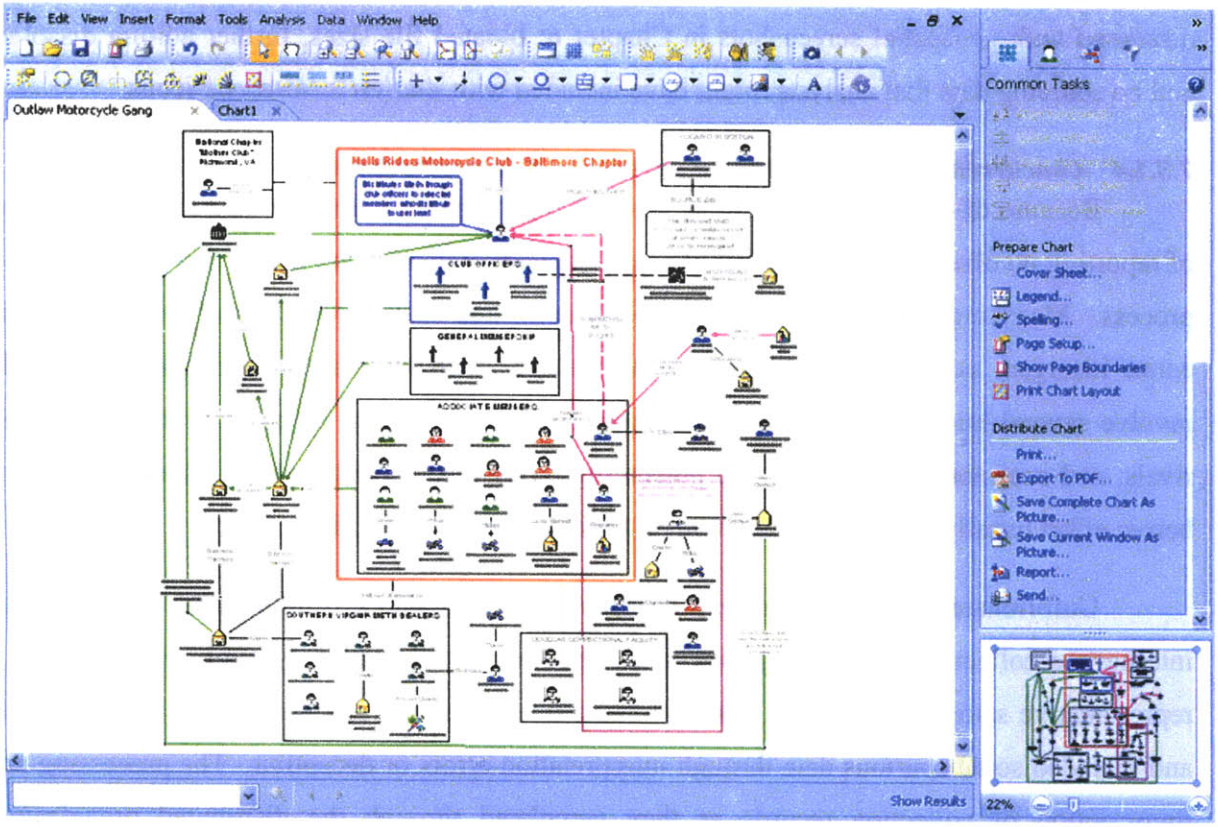


Figure 7-5: *Analyst Notebook* diagram depicting a fictitious illicit organization[43]

Automated analysis of the explicit links drawn in the diagram, or merger of the data with another network, would destroy the carefully laid-out picture. Even ambitious, multi-analyst, thousand-node graphs were usually built and arranged manually, which thus locked in minor layout and interpretive decisions. Thus most of the social networks built by forward analysts with situated knowledge of their subject and access to local reporting were not usable in all the dazzling network analysis and visualization tools built by counterterrorism contractors.

Analyst's Notebook, furthermore, had austere licensing protection,[44] so it was not universally available nor was its interface very extensible without a lot of work. Thus many users simply pasted screenshots into *PowerPoint* in order to share them, with the same problems

---

to the rectangles themselves. It's also a question about whether the *Analyst's Notebook* data model and interface are open to programmatic extension, something the application doesn't support well.

[43] This image from i2 *Analyst's Notebook* corporate promotional material fairly well reflects the style of network diagrams working analysts produce; http://www.i2inc.com/products/analysts_notebook/ [accessed 9 December 2009]

[44] A USB dongle with a valid electronic license had to be plugged into individual workstations to access the full version of the software.

discussed with geospatial screenshots in Chapter 6: bloated file sizes, further editing disabled, and no sourcing data that analysts might have included with *Analyst's Notebook* icons.

7.3.1.4 Concurrent Evolution of the Insurgency and its Representation

Because of the ontological and technical design barriers, not to mention the sheer volume of reporting involved, the construction of social network diagrams was a time and labor intensive process. Many intelligence outfits nevertheless embarked on the quixotic task of mapping the entire insurgent network in their area of operations. The local social network could easily involve several hundred active combatants and facilitators, several times as many local allies, rivals, and occasional supporters, and potentially thousands of relationships among them. The heroic effort usually produced impressive "star charts" many meters long.

Unfortunately, the resultant wall decorations were inevitably out of date. Opportunistic intelligence collection against targets worried about operational security rarely vacuumed up a representative sample. Reporting always missed insurgents and relationships in the real world and included some spurious data through interpretation errors or deception. The processing and transcription of collection records as they percolated through the distributed organization inevitably introduced further errors. Analysts then only saw a subset of this processed data because they lacked all the right security clearances or they happened to not enter the right search terms (Chapter 6 mentioned that SIPRNET search was inexplicably sluggish). Using the reports they actually accessed, analysts had to decide what to translate onto the diagram. In reading a report, they summarized a rich written narrative into a few links, nodes, and boxes. In the considerable time it took them to build diagrams, furthermore, the real network evolved through insurgent attrition, recruitment, battlefield promotion, and interventions by local governmental and tribal actors. A lot more intelligence reporting would also have been produced in the interim, but not necessarily incorporated into the diagram. Figure 7-6 illustrates how methodological problems in the construction of social network diagrams and the battlefield evolution of the real social network cause the two to diverge.[45]

[45] The "real" network is obviously itself only a representation, as there is no way to apprehend it directly in its entirety.

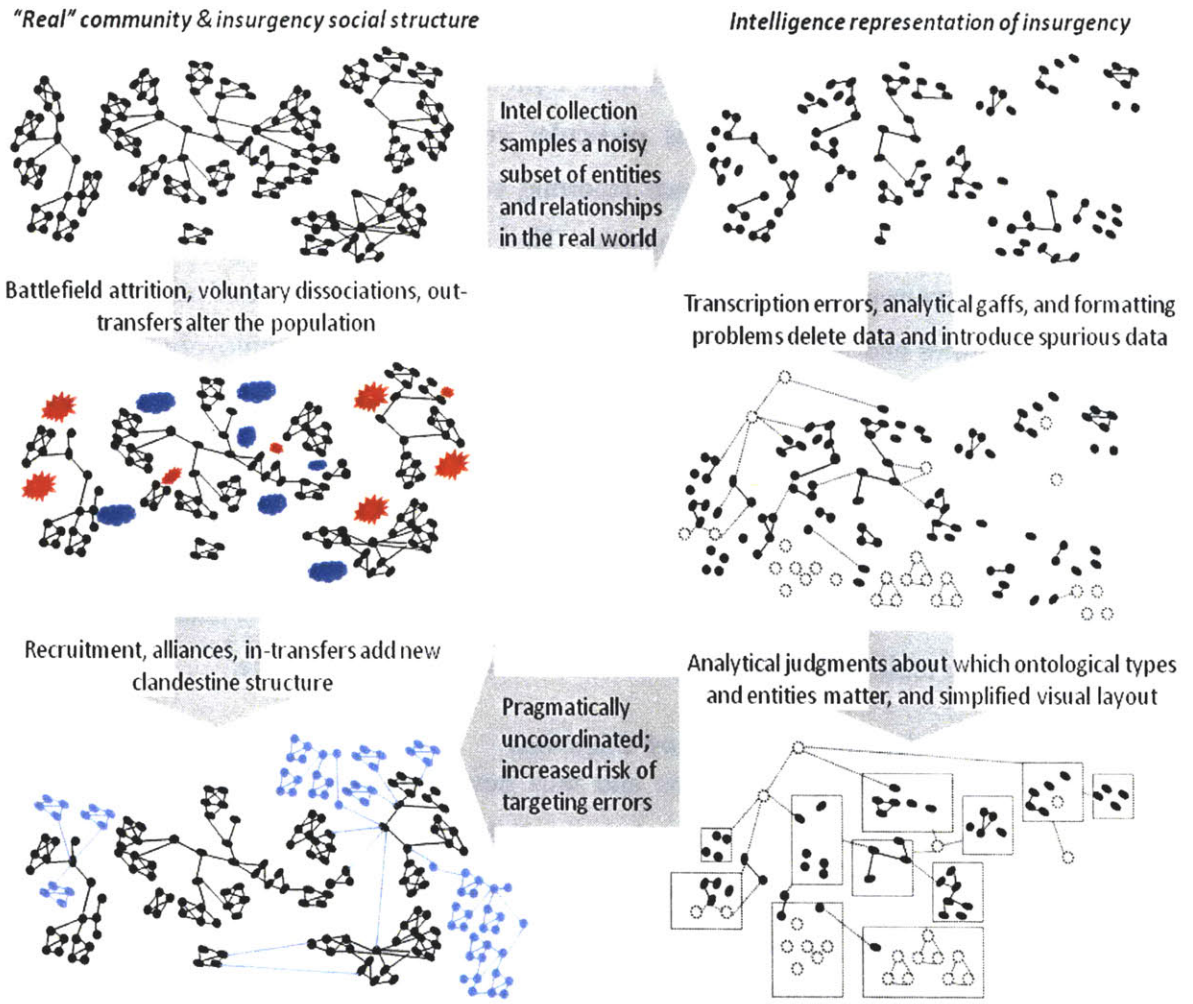


Figure 7-6: The network representation diverges from the real social network over time

7.3.1.5 Useful Scaffolding for Proscribed Problems

All of the database inconsistencies described in Chapter 6—syntactic and semantic format, primary keys, data provenance, schema discrepancy, *etc.*—affect social network data projects in spades. Different transliterations of Arabic names, the lack of any universal identifiers for targets akin to the "basic encyclopedia" numbers in strategic bombing, significant intercoder unreliability among analysts, and incompatible ontologies all seriously frustrated the aggregation of social network data.[46] As both cause and consequence of this interference friction, local analysts defected from common projects to start up local social network diagrams.

[46] To include automated social network production through automated data-mining.

In contrast to the comprehensive pretentions of "star charts" or "hairball" diagrams, most useful *Analyst's Notebook* diagrams were built from scratch by a single analyst working on a defined problem (*e.g.*, "how does this particular cell get its IED materials?"). Analysts transcribed information from intelligence reporting compiled from database searches against some starting name which they were targeting. They made ontological decisions more or less intuitively as they constructed a graphical story about a circumscribed set of people and events. They plotted entities and relationships as information struck them as intuitively relevant to the problem, rather than transcribing the entire report. Careful analysts might include citations to reporting within the diagram (which would be hidden in *Analyst's Notebook* "cards" for each icon), but this was done on an *ad hoc* basis with much provenance loss.[47] Diagrams were usually not maintained once the analyst moved on or the motivating problem receded. The act of building a diagram forced analysts to read reporting more closely, which made analysts much smarter about their topic even if the diagram itself received little further use.[48]

7.3.1.6 Rhetorical Uses of Social Network Diagrams

For analysts who built diagrams and thus developed some degree of subject matter expertise, the diagram served as a mnemonic to recall details of reporting or a briefing aid to help tell a story about a particular insurgent cell or event. The diagram could also be a rhetorical prop to make a case about why an individual "deserved" to be targeted. In contrast to the idea that social network analysis should lead to the discovery critical nodes, analysts usually built diagrams to corroborate a lead (typically SIGINT or HUMINT) that explicitly stated that a given individual was someone important.[49] In the extreme rhetorical version, the diagrams would simplistically show a few links (often the vague "associated" type) between some target and a

---

[47] If the analyst was the type who printed out traffic to read with a highlighter, exploiting the affordances of paper in order to peruse a lot of reporting on the desk while diagramming on the screen, then the analyst would be less likely to include sourcing, because then digital cut-and-pasting wouldn't be so convenient.

[48] This is an example of byproducts of report generation becoming more important than the report itself, as discussed by Martha S. Feldman, *Order Without Design: Information Production and Policy Making* (Stanford University Press, 1989)

[49] This observation pertains to network diagrams where analysts determine the ontology in their representations and used many different types of reporting. SIGINT network diagramming is something of a different animal. Traffic analysis of communications could identify previously undiscovered nodes that were important in an organization's communication networks. It could work well because the links and nodes map very well onto real world calls and phones. The ontology was stabilized through the software packages and analytical techniques that were tailored specifically to deal with that real-world infrastructure. Call chain analysis is described in James Bamford, *The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America* (New York: Anchor Books, 2008), 149.

known high-value individual in order to provide a visual argument of guilt by association. Sometimes the diagram was convincing in lieu of evidence.

Intricate "star charts" also created an aura of omniscience in the room where they hung as wall-decorations. The large printouts of network diagrams on the walls of intelligence shops were often out of date, as discussed above. Yet the wall posters had incredible longevity, often staying up through multiple personnel rotations, which meant that no one present remembered putting the picture together or what the individual links meant. Instead of providing information on the specific relationships between specific insurgents, which had already changed by then anyway, these products advertised something else: there is knowledge in here; the people who work here are smart; this is the sort of place that would know this sort of detail; these analysts have been hard at work to produce something like this; information that emerges from here is based on detailed network analysis; these people are immersed in the Iraqi situation; you can trust us. A room full of charts and maps on the wall and sprawling visualizations on monitors performatively enhanced the image of its occupants as reliable experts. This is an example of the political mobilization of centers of calculation discussed in Chapter 3.

Social network diagrams appeared sophisticatedly comprehensive and at the same time easy to understand, but at the same time they hid assumptions and transcription errors in their construction. The appearance of accuracy and thoroughness could relieve pressure on analysts to actually work hard to achieve representational validity. The reification of an "associated" link on a seductively detailed but methodologically suspect diagram might turn innocent milkmen into nefarious villains. There was great uncertainty and adaptability on both sides of the social network representational problem, objectively as the insurgency evolved and subjectively as analysts built diagrams. The numerous degrees of freedom therein constituted a threat to referential integrity, which was only lessened somewhat in cases where durable infrastructure helped to standardize link and node ontology, or where the act of constructing diagrams of well-proscribed problems fostered pragmatic coordination between local analysts and operators.

7.3.2 Packaging the Target

Counternetwork analytical methodology, as a rational ideal, begins with commander's guidance to disrupt a given clandestine organization. The map of the clandestine network is first constructed through the combination of intelligence reporting and then analyzed to discover

"high value targets" and associates who might provide further intelligence or access to them. This picture of the network suggests functional "lines of operations," such as logistics, propaganda, or different factions of the group.[50] In practice, as I have described, analysts usually built tractable partial networks around specific named personalities on their own initiative. Rather than value-free pictures of the world, diagrams were seeded around designated targets. Targeting guidance then provided a retroactive legitimation of the targets which bubbled up thusly. This raises the question of how, if not through the methodical fusion of intelligence, an individual could be designated a target in the first place.

No unit goes to war with a blank slate, certainly not four years into a war like the SEAL squadron in Anbar in 2007. The relieved squadron, conventional battlespace owners, intelligence agencies operating in the area, indigenous partner forces, tribal allies, and HUMINT sources all held opinions about who the "bad guys" were, target lists of insurgent names, and/or *PowerPoint* target dossiers on individual targets. A pool of potential targets was floating swirling around computer networks when a new unit checked in. The pool expanded as working-level analysts or operators took initiative to follow up a lead not yet on any lists from a HUMINT contact, an engagement with a local tribal figure, or a SIGINT report. The resulting *PowerPoint* file—usually copied from a previous file as a template—would circulate informally via email, show up on a SIPRNET website, or come up in conversation during the frequent person-to-person liaison among units stationed on the same base. Targets thus came from target lists and target folders, which were often copied from other people's target lists and target folders, which at some point came from someone's suspicion that somebody was a "bad guy."

7.3.2.1 Target Intelligence Package

SOTF intelligence fusion was fragmented without one comprehensive center of calculation; nevertheless, if there was any representational genre that was most situated at the apex of incoming and outgoing cascades of inscription, it was the *PowerPoint* target intelligence

[50] These counterterrorism "lines of operation" focus on functional kill-capture target sets, which contrasts greatly with the usage of the term "lines of operation" in conventional forces to describe the broader efforts of counterinsurgency or stabilization forces, such as governance, development, security force training, and insurgent combat. Counternetwork "lines of operation" thus fall narrowly into the one "kinetic" counterinsurgency "line of operation." The doublespeak no doubt makes counternetwork options seem more palatable within the counterinsurgency framework with which they stand in tension.

package (TIP), or target folder.[51] The TIP consolidated intelligence reporting and downstream fusion products (like maps and network diagrams), made the case for targeting a "nefarious" individual,[52] and would eventually support construction of a "concept of operations" (CONOP) document in order to secure headquarters permission to assault the target.

Chapter 6 mentioned that personnel used *PowerPoint* as a generic graphics package to implement a noisy ersatz database for entities with recurring data elements. Most TIPs contained a mug shot photo, bullet statements providing physical description and significance, a summary of intelligence reporting on the target, a cut-and-paste network diagram of associations with other maps and imagery of suspected locations, *etc.* (Figure 7-7 mocks up the first slide in a TIP). TIP quality and level of detail varied a great deal across targets, given that the database-like structure was maintained only by users rather than imposed by an actual database schema. It was furthermore—like so many digital products—a fusion product of fusion products. Some analysts embedded entire *Word* documents and *Analyst's Notebook* diagrams into the *PowerPoint* TIP in order to keep references together in one package.[53]

[51] Larger intelligence organizations tended to maintain target folders as web pages, while tactical units almost always had *PowerPoint* TIPs.

[52] Analysts and operators used the word "nefarious" with surprising frequency to describe targeted personalities. The word sounds serious and sinister even in lieu of actual evidence.

[53] Embedding a file rather than cut-and-pasting a screenshot preserved some provenance data and functionality in the source application, which enabled *post hoc* auditing or further analysis. It also bloated TIP file sizes.

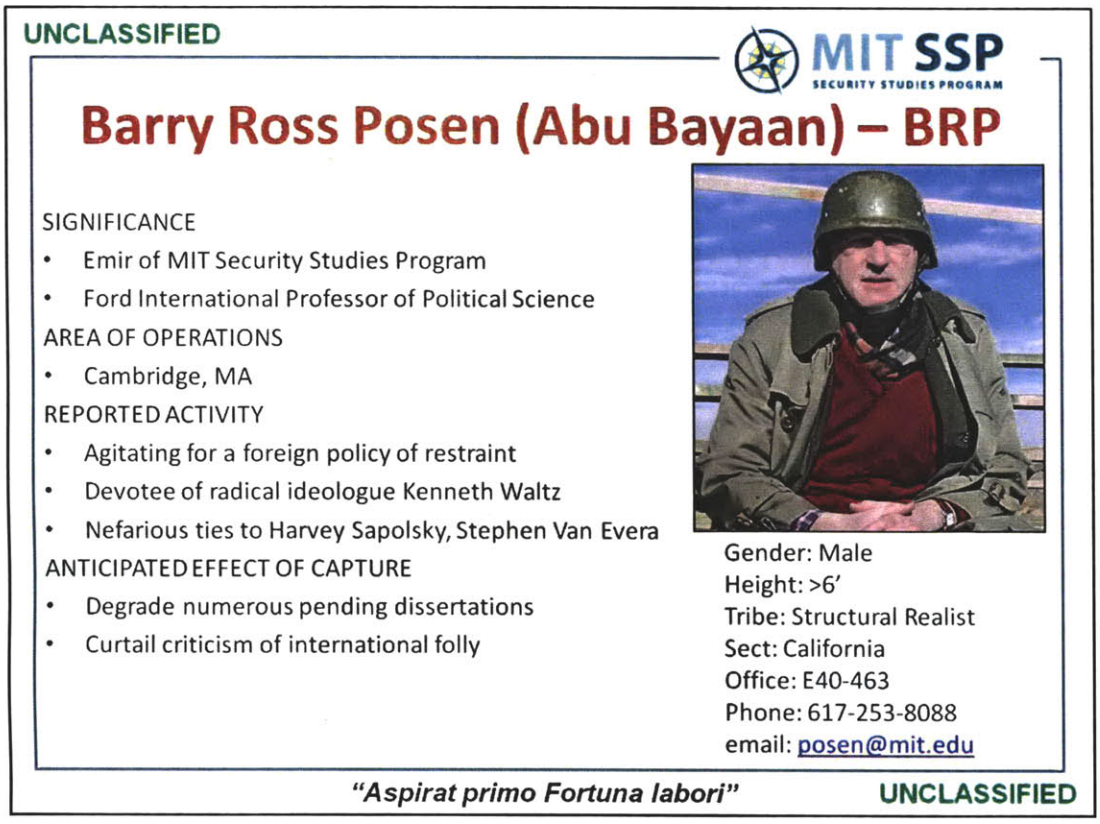


Figure 7-7: Whimsical mock-up of the first slide in a *PowerPoint* Target Intelligence Package.[54]

Intelligence personnel at the lowest echelons faced a great deal of pressure from operators to produce targets. Junior personnel, many of them reservists on their first deployment, lacked both tradecraft experience and "operator" status in the SEAL caste system. They were thus indisposed to exercise skepticism about target quality or to push back against pressure to be a team player. By providing targets, intelligence "techs" could participate in the hunt, and they could vicariously identify with the "operators" going outside the wire to catch the prey. They were disinclined to ask whether some "bad guys" were necessary evils in the local social structure (*e.g.*, a corrupt police chief with important tribal connections), whether some were potential allies if they could be persuaded to defect, or whether some were misidentified by

[54] Classification labels, the logo of the unit which produced the TIP, and a belligerent Latin logo for the unit ("Fortune favors the first attempt" in this case) would appear in the slide master template to be automatically added to every slide (thus automatically classifying them). Slide elements include the high-value individual's name, his *kunya* (Arabic for either the firstborn son or a *nom-de-guerre*; "Abu Bayaan" connotes clarity and eloquence of argument), a three-character abbreviation used in lieu of difficult-to-remember Arabic names, a nefarious-looking mugshot, identifying personal data, and summary analytical judgments.

the SOTF and not actually "bad guys" at all. The designation of an individual as a target avoided these questions by packing them up into the black box of the TIP.

7.3.2.2 Target Lists

Many units created target lists divided into categorical "tiers" with senior leadership at the top, lieutenants in the middle, and soldiers on the bottom; functional "lines of operation" cut through these tiers vertically. Names and mugshots could thus be arranged on a *PowerPoint* slide to convey a sense of relative influence among individuals, without, however, committing to depicting specific lateral and vertical relationships among them. The target list often took the place of a social network diagram. By describing only the rough contours of who was important relative to whom, but without committing as to how they were related, this representation stood a chance of remaining stable even as the real organization evolved in its details. The simplicity of the list lowered the costs of construction and maintenance in keeping it coordinated with the insurgency. Everyone on the list was usually a "bad guy" (although some might be flagged as no-strike targets for some political or intelligence consideration). Thus the product was easier to understand than a hairball network diagram.

Target lists also reinforced commando identity. One SEAL mentioned that the target list makes a good slide because it's satisfying to cross bad guys off the list when you get one. After-action reports that could claim "captured SOTF HVI #2" looked good. Movies that end with dead bad guys are cathartic, and the list clearly showed who the bad guys were. Target lists are also inexhaustible, like any good action-movie franchise, so the unit could keep doing what it was good at: whenever they got two of the ten most wanted, eleven and twelve could get promoted. Every unit had a target list, so even if they couldn't capture their own, they might capture somebody else's and thereby demonstrate commitment to "Jointness," as the bullet-point "killed 3rd Battalion's HVI #1" looked good too.

Was the target list a result of analysts poring through the traffic, of careful network analysis, and of collaboration among all interested parties? Or was it an intuitive, *ad hoc*, best-guess? Or, worse, was it just copied wholesale from some other unit's target list—or even worse, from a single HUMINT source? I saw evidence of all of these at different places and at different times, depending on the competence of and constraints on analysts in various

circumstances. In the end, the *PowerPoint* target list was another black box which didn't advertise its mode of production.

7.3.2.3 Post-Hoc Guidance

If my reader is still confused about where targets came from, then I have succeeded in conveying some of the confusion that the SOTF headquarters staff experienced upon encountering target nominations from the Task Units. Task Units often developed targets discretely to avoid being second-guessed. Sometimes the SOTF headquarters would hear about a particular target only once a Task Unit requested permission to launch a raid. The SOTF staff would then have to scramble to figure out who the target was and why the Task Unit wanted to go after him, other than the simple fact that he had been located.

The ideal targeting cycle moves from guidance to intelligence analysis of the target system to development of specific targets, but the reality usually went in reverse. Once the bottom-up workings of the targeting process are appreciated, then headquarters targeting guidance and target lists can be seen more as retroactive legitimation of activities the Task Units were inclined to pursue anyway. A guidance letter enabled the headquarters to show that it was in charge and provided a way for subordinates to demonstrate that they were obedient. There was usually enough ambiguity in the guidance letter that an enterprising Task Unit would be able to cover their preferred target (*i.e.*, the one most actionable) under it. The headquarters target list was, furthermore, balanced across the top targets of the Task Units (*i.e.*, each Task Unit had three of its top targets on the SOTF's top ten), which conferred some legitimate status on their targets without directing them against new targets or making prioritized judgments about how best to affect an insurgency which did not confine itself to the same Areas of Operation. Weekly target meetings provided the headquarters staff a window into Task Unit target priorities and TIP production (by enabling staff officers to demand information "for the commander") and an opportunity for the staff to collectively tell a coherent story about how the SOTF was fighting the war. Headquarters guidance—and headquarters reporting in general—organized the ferment of tactical activity into something more coherent and legible for public consumption.

7.3.3 Pattern of Life

Once reified on a *PowerPoint* TIP, the target *as such* was essentially put into a black box. Black boxes could be opened later, of course, should someone decide to question assumptions or

methodologies behind the initial target designation. Yet that became harder to do as the hunt gained momentum, as collection effort was invested, and as the representational residua of tracking accumulated. More machinery was in place for building up a target than for inspecting its construction. The time and effort spent going after a target reinforced a sense of the target's value. The processes for understanding and developing targets were somewhat ambiguous, as just described. The processes became more well-defined and routine as target development moved closer to action, so SOTF representational practice became more reliable.

Pattern of life is counternetwork jargon for a visual representation which renders the target's habits of communication and movement increasingly predictable. Many intelligence analysts used it as a general term for geographic maps of activity, timelines charting daily or weekly habits, or social network diagrams of frequent contacts, although some units also used the term for a specific type of graphic. A more predictable pattern of life afforded tighter triangulation of the target's future whereabouts.

The intelligence events which *fixed* a target at a location and within a given timeframe were called *triggers*. A trigger might be an extremely perishable tip on a target's movement, or it might be a reliable report that the individual would be bedding down at a safehouse on a given night in the future, allowing for more lead time to plan. Pattern of life analysis accumulated representations with the goal of developing *actionable* triggers. The same types of collection that were used to find a target (signals, spies, drone video, satellite images, reconnaissance teams, *etc.*) could also be a trigger. Full motion video from a Predator could be used over a period of days or weeks to follow vehicles associated with suspects in order to discover patterns of movement between various locations. The same type of video of the same vehicle may later be a trigger to interdict it if other sources indicated the target was going to meet the vehicle. The difference was that the accumulation of traces from many other collection events (video as well as SIGINT and HUMINT) changed the context of the video. The trigger is that line of collection which makes an intersection with the target more reliable, within the parameters of risk the SOTF was willing to accept and rules of engagement it had to obey.

The SOTF's information system was organized to produce tactical triggers rather than high-quality targets. The integration of perceptual data from many streams occurred on various computer screens, consolidated in *PowerPoint* target folders and lists, and culminated in triggers.

Operators took more interest in intelligence at this point because they wanted to improve the reliability and frequency of triggers. Frequent triggers provided more targets to assault. Reliable triggers ensured that targets would be on the objective when the assault team hit it. Reliability did not refer to the quality of the target, an intelligence fusion problem of less interest to operators. The identity of the target *per se* had been established by the creation of a target folder and investment of effort in the hunt. The trigger simply rendered the target *actionable*. Triggers were the culmination of integration because they began the articulation of raids.

To sum up the SOTF's integration phase, centers of calculation were fragmented across many different computers and files, although the target folder did provide some focal point for fusion. Abstractions, especially social network diagrams, were leaky and prone to become uncoordinated with the environment. Several types of representations, notably target lists and network diagrams, often played rhetorical roles to sell targets and to reinforce the identities of both special operators and intelligence personnel by suppressing questions about their construction. The substantial friction throughout the integration phase was masked by its packaging into an actionable trigger. The ideological consistency of the SOTF's target fixation covered up the interference friction with insulation friction.

7.4 Articulating Raids

The articulation phase of control moves from information processing in disconnected centers of calculation to reconnection with the environment. Perception transforms physical contact into movable symbols, but articulation works in reverse to translate symbols into more and more particular material situations. Furthermore, each physical contact with the battlefield is also an opportunity for further perception and feedback.

Articulation includes the Hollywood phase of special operations targeting. SEALs were the stars of the movie, and the SOTF audience watched them onscreen, through the video image of an unmanned Predator piloted from Nevada. Information processes were most reliable in support of the tactical operations at the core of the SEAL organization. More friction emerged as operations pulled back into the next iteration of the control cycle, which involved the removal of information and detainees from the target objective for exploitation and further target analysis. IT amplified the performance of tasks closer to the essence of the organization but did not automatically improve more peripheral tasks.

7.4.1 Mission Planning

The *full mission profile* is the central ritual in the cult of the frogman: insertion of operators into the target area, infiltration to the objective, actions on the objective, followed by exfiltration and extraction back to safety. The SEAL community in general and the SOTF in microcosm were designed around its reliable performance.[55] With the target and objective identified—and essentially exogenous to mission planning—the logistic planning for infiltration, actions on the objective, and exfiltration was a well-rehearsed drill.[56]

Mission planning began with a trigger, either from intelligence or a target passed from the Marines or other government agency.[57] An impromptu planning session among platoon leadership determined feasible options for a mission profile. Intelligence personnel scrambled to get information on the *target* (a person) and the *objective* (a location) if it wasn't already in the target folder, emphasizing tactical features like the terrain and physical layout of the house, appearance of the target and other people, threats along the route and on the objective, makeup of the local urban terrain including bases, police, hospitals, *etc.* Some of this information would be printed out on standardized "baseball cards"—similar to pilot kneeboard cards or a quarterback's play card—so that operators could carry it with them to the objective. Many mission planning products never left the executing unit. Some tactical intelligence products could be produced through "reach back" organizations like the Mission Support Center in Coronado, California because their extremely stereotyped nature created a stable communication channel: little local SOTF knowledge or customer-producer coordination was required to draw on stabilized maps

---

[55] The "theory of special operations" in William H. McRaven, *Spec Ops: Case Studies in Special Operations Warfare Theory and Practice* (Novato, CA: Presidio Press, 1995) focuses exclusively on the direct action mission profile: "All special operations are conducted against fortified positions," he writes, neglecting the unconventional warfare, persuation/psychological operations, and foreign security force training that is the bread and butter for many US SOF. Vice Admiral McRaven (SEAL) became commander of JSOC in June 2008 when General Stanley McChrystal moved on to Afghanistan.

[56] The SOTF's forward location in Anbar abrogated the need for insertion and extraction.

[57] Marine battalions sometimes handed off actionable targets to SOTF Task Units with little advance notice. This raises the question of why the Marines did not action the target themselves, as bringing in a quality high value individual would bring accolades for themselves. The target might be passed at the action-officer level by a frustrated Marine unable to get the target approved through the Marine chain of command. SOTF autonomy from the Marines provided an attractively expedient route to getting the target. The Marines might also be looking for the SOTF to play "bad cop" to the battalion's "good cop," as Marines were more involved in working among local Iraqis through daily patrols and projects. Blaming "Special Forces" protected the Marines somewhat (but only somewhat) from the backlash of rolling up a questionable target. From the Task Unit perspective, taking care of the Marine's target helped to build up relationship capital to nurture the flow of intelligence and other support upon which the SOTF depended heavily.

and databases in support of a generic mission profile. On the left of Figure 7-8 is a visibility analysis of what terrain can be seen from a given observation point; on the right is a meteorology chart assessing weather impacts on different vehicles. [58]

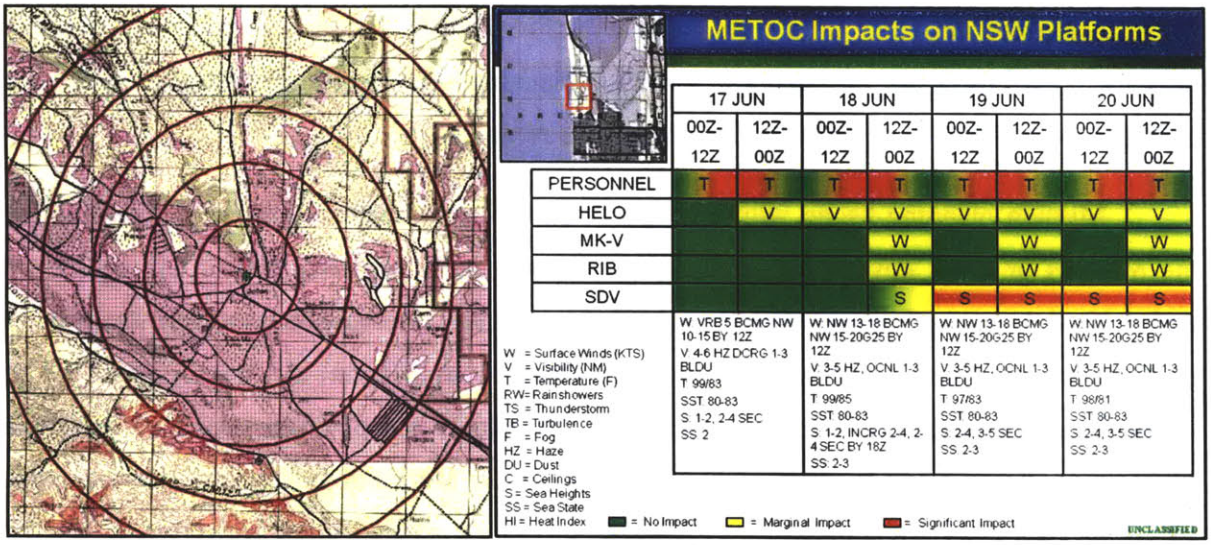


Figure 7-8: Mock tactical support products from the Naval Special Warfare Mission Support Center

The Task Unit generated a standardized "concept of operation" (CONOP) document containing a very short justification of the target's significance, location of the objective, composition of the assault force (both U.S. operators and Iraqi partners), air mobility plan, communications plan (radio frequencies and callsigns), quick response force plan pre-coordinated with the local Marine battalion in case of emergency, *etc.* The Task Unit was required to file a CONOP in both *Word* and *PowerPoint* versions so that it would be easier for staffs at the SOTF headquarters and higher headquarters (CJSOTF) to brief it, an instance of headquarters offloading its own redundant information processing onto subordinates.

Each CONOP had an *information operations* (IO) statement as to the expected effect of the mission and perceptions that Iraqis might have as a result. The IO statement was almost always a vague *pro forma* statement about disrupting the insurgency and sending a message, content unspecified. The IO statement varied little from CONOP to CONOP, a testament to the lack of attention to targeting effectiveness compared to tactical performance.

[58] "US Naval Special Warfare: Implementing Network-Centric Concepts," unclassified *PowerPoint* file, November 2003

7.4.2 Negotiating Approval

The SOTF headquarters' first notification of an actionable target was usually a telephone call from the Task Unit followed by a CONOP via email. Mission approval rested at different echelons depending on the risks and sensitivities of the operation. Routine convoys and meetings could be approved by the Task Unit, with a CONOP copied to headquarters, while direct action missions required at least SOTF approval, and those with particular risk or political sensitivity, such as the entry of a mosque, would require higher approval. To secure approval of the mission, ISR coverage, and assault airlift if necessary, there was a great deal of negotiation and coordination up and down the chain of command. In contrast to popular perceptions of top-down military command and control, Task Units were entrepreneurial advocates for their targets.

The CONOP thus became a forum for shaping staff perceptions. A CONOP that arrived from the Task Unit at the same time—or even before—a target folder gave the SOTF staff less time to evaluate the actual value of the target, creating pressure to push through approval. Task Units were also prone to abusing "time sensitive target" processes to send CONOPs at the last minute in order to get an expedited approval, even if they had reasonably known for hours or days ahead of time that they were planning against an objective for that evening.[59] Headquarters could intervene by disapproving CONOPs or placing conditions on their approval. CONOPs were very rarely disapproved on the basis of intelligence quality alone. Concerns that targets might not be important insurgents, or that hitting them would be counterproductive within the local community, were often perceived as second-guessing the Task Unit on the ground and frowned upon in special operations culture. The exception was a concern about "dry holes," which are objectives where the target flees prior to the raid or never arrives in the first place. Too many false alarms looked bad on higher-headquarters statistics.[60] While relatively little attention was given to target validation, the operations staff scrutinized missions in terms of risk

[59] In the other direction, the SOTF headquarters sometimes pressured a Task Unit to ask and plan for air support even though the Task Unit didn't want it. The Task Unit in the West of Anbar rarely requested helicopter insertion because the distances from the central special operations helicopter base out to the units in extreme western Anbar made it difficult for the birds to fly out, conduct the mission, and get back before dawn. The SOTF headquarters wanted CJSOTF to base a detachment of helicopters out at Al Asad Airfield to reduce the flying time, but to make that case, they had to show that there was a strong demand for them in a paper trail of unmet air requests.

[60] The SOTF had to negotiate with CJSOTF for air support and ISR (which meant taking these high demand, low density assets away from other regional SOTFs), and expending these on dry holes made it harder to get them for future missions.

to personnel. *Operational risks* of tactical fiascos outweighed *intelligence risks* of bad targets. The problem is that these were not neatly separable categories: a bad target could be a trap, say if HUMINT collectors took the bait from a malicious agent trying to lure a team into a booby-trapped house.

One of the SOTF's primary missions in addition to counternetwork targeting was the training of Iraqi military and police partner units. Many SEALs tended to view the Iraqis as an excuse to get outside the wire and operate, rather than viewing the training as the main effort. The training mission thus provided the Task Units an argument to get poor-quality targets approved in cases where the SOTF headquarters might push back, because the Task Unit could argue that the low quality target was an useful "confidence mission" for training their partner.[61]

7.4.3 Unmanned Overwatch

Once launched, the assault force communicated with the Task Unit via encrypted tactical radio. The Task Unit in turn communicated via SIPRNET chat with remote ISR operators to provide overhead surveillance of the raid.[62] ISR provided an unobtrusive scout which could scan the target area for threats, follow "squirters" who attempted to flee, guide the assault force onto fugitives, and monitor the target area after mission completion.

7.4.3.1 Prior Plans Coordinate Distributed Action

The assault force and the Task Unit maintained coordination through an integrated framework structured by the CONOP, shared maps, and a communication plan with *prowords* keyed to tactical milestones or contingencies.[63] Prowords, projected on a wall or printed out for ready reference in the Task Unit operations center, provided a shared script for the operation so that the assaulters on the ground could efficiently communicate their progress along predefined waypoints (insertion, rendezvous, setting security around the objective, objective secure, *etc.*), or movement to a different branch of the plan (because of troops in contact, explosives discovered

---

[61] To check the preference of units for conducting direct action missions, CJSOTF levied a requirement that there be a minimum two-to-one ratio of Iraqi personnel to SOF operators on any given mission. This limited the range of missions the SEALs could conduct (because of the larger force footprint and lower proficiency of Iraqi partners) even though there were benefits (putting a less-offensive Iraqi face on raids, incorporating native speakers, and most importantly, training Iraqis to take over security operations).

[62] Direct communication between the Task Element commander on the ground and the UAV operator was possible in principle, but usually the Task Unit handled ISR.

[63] "Procedure words" are standardized in advance of operations to streamline radio communication and provide a modicum of security.

on the objective, *etc.*) which might require additional Task Unit action (such as activating the Marine quick response force, coordinating close air support, *etc.*). These planning representations—exercised, coordinated, and studied in advance—provided tools for orienting the attention of the Task Unit commander and ISR officer as they monitored the mission unfolding on radio traffic and the ISR video. In controlling ISR in particular (through chatroom instructions to the UAV operators), the Task Unit not only responded to requests for information from the assaulters, but also proactively moved the camera focus and zoom around the objective area in order to build and maintain situational awareness at the Task Unit. They actively followed along because they had real and potential inputs into the unfolding tactical action. Although remote from the raid site, these personnel were part of a tactical feedback loop, so the ISR representations had pragmatic meaning by cuing appropriate action. This is an example of how prior plans, shared among distributed actors, structure real-time situated performances.[64]

7.4.3.2 Kill TV

Unlike the Task Unit with its active tactical inputs, a larger passive audience played a more vicarious role. Most ISR video streamed over the SIPRNET. SOTF headquarters personnel could subscribe to a feed and project ISR data and chatroom conversations on the wall of the operations or intelligence centers, or they could watch it on a monitor at their desk. ISR video was colloquially known as "kill TV" in reference to infrequent moments of combat excitement.[65] The sobriquet conveys the extent to which full-motion video provides a sense of intimate participation in combat without the personal risk and thereby transforms war into infotainment for many participants. ISR video was projected right beside a satellite television displaying either news programs or sports, contributing to the discordant sense of normalcy which distinguishes staff life even in the midst of combat operations. The unfolding mission provided an alternative to Fox News,[66] as well as a way of vicariously identifying with the heroic

---

[64] Lucy A. Suchman, *Human-Machine Reconfigurations: Plans and Situated Actions, Revised Edition* (New York: Cambridge University Press, 2006)

[65] Most mission activity consisted of troops patrolling to or from the objective or walking around while the site was secured and exploited. Generally, but certainly not always, only the initial entry onto the objective held potential for combat action. SOTF personnel wandered into the TOC to watch the video out of curiosity and then wandered away if there didn't seem to be much going on.

[66] The right-leaning news coverage of the *Fox News Channel* was the preferred channel on television sets in military offices and dining halls. Televisions were almost perennially on in operations and intelligence centers, and they often captured the attention of personnel. I heard the term "FOX-LOC" for "Fox News-induced loss of consciousness," a play on the aviation term G-LOC for acceleration blackout. I visited one TOC where the

image of operators on the ground.[67] The allure of virtual battlefield presence was strong. Senior officers were hardly immune, and a number of writers have commented on the tendency of ISR video to occupy leadership with tactical matters below their pay grade.[68]

As the name implies, "kill TV" footage has graphic potential. This is especially the case for close air support platforms like the AC-130 Specter gunship, which could be on call to monitor and if necessary provide supporting fires for SOTF operations. Full-motion video unquestionably improves the accuracy and responsiveness of close air support, reducing (but not eliminating) fratricide and collateral damage risks. By removing the observer from personal risk, it can also improve cool-headed judgments. An undesirable side effect, however, is that some personnel indulged a vicarious bloodlust or morbid fascination when they obtained sensational video and emailed it around to their buddies (on SIPRNET, but also on the open internet on occasion). Such emails enhanced warrior prestige by signaling proximity to martial activities by virtue of access to graphic material. Remote video and the ease of sharing it buffered out the personal risk, fear, and empathy which have helped to moderate violence fetishes in traditional combat. Many of the organizations which generate this material came to recognize these dangers and implemented strict controls on its dissemination. Soldiers throughout history have experienced natural aversions to killing as well as intoxication with violence, so it should not be surprising that the remote experience of killing ranges from sober technocratic earnestness to video game pathology.[69] Contemporary wars are uncontrolled experiments in the moral and psychological effects of vicarious killing, and an area which deserves closer study.

---

intelligence officer had intentionally pointed his analysts' desks away from the ISR and news feeds in order to keep them focused on target analysis.

[67] SOF has a strong martial culture, but as its fundamental maneuver units are small teams, combat leadership opportunities peter out above the company grade level (SEAL platoon or SF ODA). ISR video could provide more senior leaders with a sense of being once again involved in the battle, tempting them to intervene in or request too much information from ongoing operations.

[68] See, for example, Hy S. Rothstein, *Afghanistan and the Troubled Future of Unconventional Warfare* (Annapolis, MD: Naval Institute Press, 2006), pp. 132-137; Singer, *Wired for War*, pp. 344-359. Singer coins the term "tactical general" as the ironic inverse of the Marine Corps' concept of the "strategic corporal," who may cause far reaching effects for good or ill through his tactical decisions.

[69] Joanna Bourke, *An Intimate History of Killing: Face-To-Face Killing in Twentieth-Century Warfare* (New York, NY: Basic Books, 1999); David Grossman, *On Killing: The Psychological Cost of Learning to Kill in War and Society* (New York, NY: Little, Brown & Co, 1995); James Hillman, 2004, *A Terrible Love of War* (New York, NY: Penguin Books); Chris Hedges, *War is a Force That Gives Us Meaning* (New York, NY: Random House, 2003)

7.4.4 Battle Tracking

In discussions of command and control, the visualization of battlefield operations, which enables headquarters monitoring and control, is often described as a "common operational picture." The god's eye view includes the *Blue Force Tracker* (BFT) plot of friendly forces and corresponding intelligence overlays of enemy locations derived from ISR. The everyday pragmatic "common operational picture," however, was not common because not everyone was on the same email distribution lists or able to access the same share drives, and some SOF units opted out of BFT. It was not really operational because electronic displays often aggregated at too high a level to represent fluid developments on the battlefield and omitted irregular combatants, and because the SOTF emphasized administrative recordkeeping over linking mission goals to tactical assets. Nor was it much of a picture, for data was scattered across many different types of media, and abstract icon graphics only picked out selected rough features of the ground situation. Specific technical tools like BFT oriented awareness and cued further information collection, but they were only accurate to the degree that complex systems could be rationally engineered to make the elements of the display commensurable.

7.4.4.1 Blue Force Tracking

BFT worked by broadcasting the GPS-derived coordinates and identity of a tactical unit over an encrypted circuit so that an icon of the unit could be plotted on a digital map (such as *FalconView*) to aid coordination of friendly maneuver, headquarters battle tracking, and to prevent fratricide. BFT enabled an improvement in speed and accuracy over figuring out locations by map and compass, passing coordinates by voice over radio, and plotting them on a map. BFT worked relatively well because its engineering requirements were clear; there was a general consensus on the desirability of BFT; and the icons on the screen reliably picked out features of the world, namely the BFT transmitter itself, which was usually correlated with the unit it identified. BFT was not a panacea for situational awareness, however, for the referential integrity of the icon to troops on the ground could be broken: the signal was degraded by urban clutter and transmitting beacons could fail; the icon aggregated the entire unit rather than individual troops, so the display could mislead careless observers into believing dispersed personnel might be more concentrated than they in fact were; some clandestine missions opted not to broadcast their location to the common circuit. The absence of an icon on the map did not, therefore, necessarily mean an absence of troops on the ground. Nevertheless, most parties

recognized more advantages than disadvantages in BFT, which should be considered one of the clear success stories of the RMA.[70]

7.4.4.2 Bureaucratic Scaffolding of Tactical Operations

The dream of integrated collaborative mission tracking was not so successful. SOCOM had a system called "Command Post of the Future" into which the SOTF operations watch was supposed enter data so that the entire chain of command might view mission status on a map; the system took up an entire table, but like so many military IT efforts, it sat there unused. SOTF personnel defaulted instead to Microsoft *Office* products, which they found both more reliable (everyone had access to an *Office* installation) and easier to tailor as new data tracking requirements emerged or they needed to make notes on mission idiosyncrasies. While the SOCOM system's architects focused on rationally capturing data, the SOTF focused on capturing targets, which was a less-than-rational process which entailed more paperwork, briefing graphics, and coordinating emails and phone calls than the narrow engineering focus on mission tracking data could accommodate. The regular disuse of military command and control systems attests to the importance of situated, tacit, changeable knowledge in the practice of command and control.

The SOTF headquarters passively monitored mission progress with little active input outside of responding to some unforeseen disaster. The SOTF instead managed the bureaucratic scaffolding for missions and fielded queries from higher headquarters. "Battle tracking" in practice meant copying files emailed from the Task Unit into a share drive folder for each mission, and updating an *Excel* spreadsheet called "the mission tracker" with the receipt times of each product, times of major milestones, and some basic data like the number of friendly and enemy casualties if any. The mission tracker surprisingly contained no fields directly linking the mission to target—such as even the target name—and little data concerning mission outcomes, another indication of the SOTF's overriding focus on the safe performance of the full mission profile rather than connecting missions to targets to effects in the world. Following the completion of the mission, the Task Unit would forward a short "Quicklook" *Word* document

[70] Michael M. Sweeney, "Blue Force Tracking: Building a Joint Capability" in *Information As Power, Volume 3*, ed. Jeffrey L. Caton, Blane R. Clark, Jeffrey L. Groh and Dennis M. Murphy (Carlisle Barracks, PA: United States Army War College, 2009): 107-126.

describing the outcome and any significant activity on the mission. A more thorough operations summary would follow later, along with a graphic "storyboard."

7.4.4.3 PowerPoint Trophies

A *PowerPoint* storyboard became the digital trophy of a successful manhunt. Storyboard slides described the mission objective, target significance, and composition of the force; a map of the objective area; and pictures of any killed or captured individuals and recovered weapon material. The pictures included brightly-colored labels (using *PowerPoint* "WordArt") for each mugshot of a "Jackpot" (target captured) or "PUC" (a "person under control," or detainee). The more spectacular the mission—that is, the more it conformed to commando archetypes, either heroic or tragic—the more detailed the storyboard. Storyboards were emailed out to the wider SEAL community back in the U.S., and they would go on to form the core of the squadron's after action briefs. Storyboards reinforced the commando identity by providing evidence of ongoing heroism and seeds for further discussion and learning.

7.4.5 Feedback

Every articulation into battlefield contact enables further perception and feedback. The intelligence-generation aspect of the raid transformed a combat zone into a crime scene. Processes for evidence transportation, forensic analysis, detainee processing, and reporting rendered a chaotic forward contact increasingly legible to a disconnected center of calculation. In keeping with the bias toward commando action, the SOTF performed actions on the objective, in which intelligence enabled operations, with more finesse than the follow-through exploitation of material, in which operations enabled intelligence. The exploitation of recovered media and detainees was seen more of a cleanup requirement following a successful raid, rather than the intentional set up for follow on raids. Exploitation dealt with the detritus of past operations and was not well-integrated into active target development.

7.4.5.1 Evidence Collection

Weapons, equipment, documents, and other things on the objective could have intelligence value for hunting other insurgents as well as evidentiary value for convicting detainees in Iraqi courts. The evidentiary justification of *sensitive site exploitation* usually appealed to operators more than the intelligence gathering purpose: a guilty prisoner sent to long-term detention justified the risk of the raid and resonated with the heroic narrative of the mission.

The SOTF legal officer (JAG) took the lead in encouraging the Task Units to perform more thorough site exploitation, a law enforcement skillset not common in military units (reservists with police experience were generally not taken on missions because of the "tech" stigma). Intelligence collection for follow-on analysis was thus a byproduct of evidence obtained for conviction.

Items like documents, cellular phones, and computer media constituted formalized records of the insurgents' previous interactions with the world, but operators had to first recognize them as valuable enough to collect out of the large amount of printed or digital material to be found in any house (avoiding overzealous collection that might be interpreted as theft), and then to transport media without corrupting it along the way.[71] Some media could be forensically exploited by technicians on the objective or back on base who could then inject intelligence records back into the targeting cycle. Unfortunately, the files and documents that could best illuminate the inner workings of a clandestine organization were essentially inaccessible to the SOTF because of the Arabic language barrier and the volume of documents.[72] Document exploitation is painstaking work because the same type of clutter, redundancy, and triviality on the SOTF's hard drives plagued the insurgents' as well! The task far exceeded the time and effort constraints of forward-deployed analysts who were the most familiar with the target's activities and thus best able to identify relevance. Thus the processing, translation, reformatting, and examination of captured media by intelligence analysts in the U.S. without a situated feel for what was important might be delayed for weeks or months, and much would remain unexploited for years if at all.[73]

Anbar was fortunate because the Marine Corps Intelligence Activity based in Quantico, Virginia could undertake long-term document analysis while maintaining a current

---

[71]William G. Perry, "Information Warfare: Assuring Digital Intelligence Collection," Joint Special Operations University Paper 09-1 (July 2009)

[72] Unlike popular conceptions of insurgent and terrorist organizations as leaderless, formless networks, they often turn out to be quite bureaucratic in character. Al Qaida in Iraq (AQI), for example, had standardized forms for enrolling suicide bombers, for approving temporary leave outside of the country for recreation or medical treatment, or for permanent disaffiliation with the organization, as well as accounting spreadsheets for managing corporate finances, personnel records, and intelligence sources; Brian Fishman, *Bombers, Bank Accounts, and Bleedout: Al Qaeda's Road in and Out of Iraq* (West Point, NY: Center for Combating Terrorism, 2008)

[73] The bureaucratic architecture of US national-level document and media exploitation is described in: Director of National Intelligence, "Intelligence Community Directive 302: Document and Media Exploitation" (6 July 2007), http://www.dni.gov/electronic_reading_room/ICD_302.pdf

understanding of detailed empirical context by rotating its analysts through forward positions. This is another example of successful reach-back support, but in this case the communication was stabilized not through stereotyped products as with Mission Support Center's tactical graphics, but through the cultivation of personal relationships among Marines, deep analytical expertise with long-term focus and some methodological rigor, and a common understanding of the operational problem.

7.4.5.2 Turning Detainees into Data

Tactical questioning on the objective and interrogation in a detention facility are overt forms of HUMINT collection.[74] They were subject to the same problems of equivocation at the source, communication through an interpreter, and bias toward actionable targeting intelligence discussed in the section on perception above. Unlike the HUMINT priesthood, however, interrogators (known as "gators") did not enjoy the same oracular status. The black art of knowledge extraction was tainted with the opprobrium of prison, so interrogation was seen as a necessary evil rather than a respectable profession. SOTF interrogators essentially worked on their own, which kept them busy and disassociated with target development or analytical support for their labors. Furthermore, operators perceived interrogators less as part of the hunt leading up to a dramatic raid and more as auxiliaries who helped with the clean up, as evidenced by a general unwillingness to include "tech" interrogators on missions, where the shock of capture was more conducive to eliciting actionable information then a detention facility.[75] Rather than an indispensible source of feedback and follow-on targets, interrogators tended to be marginalized from both operational and analytical efforts.

The process of making detainees legible for analysis began on the objective by tying on capture tags with basic information like name and date. Further records began to accumulate

---

[74] "Tactical questioning" refers broadly to informal interviews of local people by military personnel, using direct questions (who, what, where, *etc.*), in the normal course of patrolling or conducting an operation. Adversarial interrogation features indirect manipulation and specialized approaches which require lengthy training and certification and can only be conducted in controlled detention facilities under U.S. military regulations. Both are subject to the law of armed conflict prohibiting torture.

[75] As commandos burst into a house and neutralized threats, suspects on the objective found themselves facedown on the ground with their hands zip-tied. Fearing for their lives—as a natural byproduct of the raid, not of any intentional interrogation approach—prisoners were more likely to respond to direct questions with veracity than after an opportunity to compose themselves in captivity. Even if direct questioning provided no information of obvious value, their responses (or lack of responses) allowed 'gators to begin to triage detainees for expected intelligence utility and to develop interrogation approaches.

during in-processing at a temporary holding facility, to include a medical examination, biometric samples (fingerprints and retina), and more direct questions. Operators drafted "shooter statements," which were signed legal depositions of their recollections of events on the objective, and they were supposed to debrief with interrogators about each detainee. Detainees, their effects, and their files would be transferred within a few days to a more robust regional detention facility operated by Marines, where they would undergo yet more processing. The entire detention process was heavily regulated by the law of war, specific Defense Department directives, and service doctrine. One irony is that the penal controls in place to prevent the sort of abuse made notorious at Abu Ghraib prison also made it more difficult for skilled interrogators to run the soft approaches that were generally more effective: it is hard to convince someone in manacles and prison garb, confined to a prison cell and an interrogation booth, of friendly intentions.[76]

As with HUMINT source meetings, interrogation reports usually omitted colorful information that the interrogator elicited instrumentally to get at more narrow intelligence about the insurgency. The detainee was quite literally a captured ethnographic informant,

---

[76] The popular conception of interrogation among non-interrogator military personnel as well as the larger television-viewing population is that it involves abusive, hostile confrontation, just as agent Jack Bauer of the series *24* is often successful in extracting actionable intelligence from terrorists through torture. Most professional interrogators recognize, however, that more seductive approaches which leverage an emotional connection with the detainee often prove more effective. Good interrogators must have a lot of skill, empathy, and patience in order to build respect and rapport and to manipulate hope and pride. The most thorough public study of interrogation effectiveness is: Intelligence Science Board, *Educing Information: Interrogation, Science and Art* (Washington, DC: National Defense Intelligence College Press, 2006). For accounts of contemporary U.S. military interrogation operations, ranging from professional and empathetic to incompetent and sadistic, see: Chris Mackey and Greg Miller, *The Interrogators: Inside the Secret War Against Al Qaeda* (New York, NY: Little, Brown and Company, 2004); Alexander and Bruning, *How to Break a Terrorist*; Eric Maddox and Davin Seay, *Mission: Black List #1: The Inside Story of the Search for Saddam Hussein* (New York, NY: HarperCollins, 2008); Moazzam Begg, *Enemy Combatant: My Imprisonment At Guantanamo, Bagram, and Kandahar* (New York, NY: New Press, 2006); Tony Lagouranis and Allen Mikaelian, *Fear Up Harsh: An Army Interrogator's Dark Journey Through Iraq* (New York, NY: Penguin Books, 2007). Good historical examples of innovative rapport-building approaches with captured enemies that are nearly impossible under contemporary penal regimes—to include relocating detainees from prison settings, interrogators living with their targets, and releasing prisoners released to spy on former comrades—are described in: Stuart A. Herrington, *Silence Was a Weapon: The Vietnam War in the Villages* (Novato, CA: Presidio Press, 1982); DeForest, *Slow Burn*; Raymond T. Toliver, *The Interrogator: The Story of Hanns Joachim Scharff, Master Interrogator of the Luftwaffe* (Atglen, PA: Schiffer Publishing, 1997); Riley Sunderland, "Antiguerrilla Intelligence in Malaya, 1948-1960," RAND Memorandum 4172-ISA (Santa Monica, CA: September 1964). U.S. military interrogation policy and approved approaches are covered in: Department of Defense Directive 3115.09, "DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning" (Washington, DC: 9 October 2008), http://www.dtic.mil/whs/directives/corres/pdf/311509p.pdf; U.S. Army, *Field Manual 2-22.3: Human Intelligence Collector Operations* (Washington, DC: 6 September 2006)

knowledgeable about his local society, tribal organization, neighborhood structure, and the workings of the small slice of the insurgent organization in which he was involved. Such data constituted invaluable empirical samples for building a theoretically-informed profile of the local roots and logic of violence. Moreover, since much of this type of background information didn't bear directly on actionable intelligence that would incriminate comrades, many detainees would be more likely to answer it truthfully in order to stay away from more incriminating topics. Good interrogators usually *did* ask a lot of background questions during their many hours with a prisoner, to keep detainees talking if nothing else, and they certainly probed the detainee's motivations for joining and his disposition within the insurgency because an understanding of his motivation was usually necessary for breaking the detainee's resistance (*i.e.*, to manipulate his love of family or desire for revenge against Shia usurpers). The elicitation of societal background, demographic, and personal information was a means to getting to the more tactically-useful names, locations, and tactics the interrogator was after. Much rich data never left the booth, as tactical interrogation reports included mainly just details on specific insurgent organizations and operations, which it was the tactical interrogator's job to extract.[77]

Operators took the mission to be successful by virtue of recovering detainees in the first place, whether or not the detainee had valuable information or not. The attitude was that if they had risked their life to get someone off of the objective, then he must be guilty: "why would we go get this guy if he didn't know anything?" If the detainee wasn't giving up useful information, they often concluded that it must be the interrogator's fault: a more skilled 'gator surely would have broken the detainee and extracted actionable intelligence.[78]

Further exacerbating the problems of detainee selection and processing bias, the metrics for interrogation metrics framed success in terms of conviction rates rather than targeting

---

[77] These problems can be corrected through interrogator training and emphasis on the importance of collecting background data, but as important is including dedicated analysts observing the sessions to assist drafting reports and crafting questioning approaches.

[78] The potential innocence of detainees was a sensitive topic for the SOTF, for it called into question the judgment of HUMINT collectors, Task Unit target development, and of the operators on target who captured the detainees. There were incidents of controversy during which operators accused interrogators of being too inexperienced (or too empathetic) to be effective, but they rarely asked into the incidence of detainees who knew nothing in the first place, which would have to be attributed to flaws in target development or execution rather than interrogation. These episodes recalled the search for non-existent weapons of mass destruction which helped to justify the Iraq war in the first place, echoing Defense Secretary Rumsfeld's nostrum that "absence of evidence is not evidence of absence."

effectiveness, and took little account of the radicalizing effects of incarceration in contributing to insurgent manpower.[79] A process which should have provided a fundamental feedback on the quality of, and new inputs for, the targeting cycle was instead an auxiliary protocol to finish off a mission by sending the detainee off to long-term detention.

To sum up the SOTF's articulation phase, information processes supporting the tactical performance of raids were more robust than the staff and intelligence processes we've traced in other sections. IT usage amplified the performance of the core SEAL function, the full mission profile, so much so that representations were used rhetorically to secure permission to perform them and to celebrate them with *PowerPoint* trophies. Expedient adaptation of Microsoft *Office* software provided the bureaucratic scaffolding for raid performance where official systems broke down. Enterprise systems like blue force tracking did perform well because their requirements were fairly well stabilized and universally appreciated. As the articulation phase transitioned into perception, there was far more equivocation, as feedback processes of site exploitation and interrogation were more peripheral to core SEAL tasks.

7.5 The Insulation Variety of Information Friction

The previous sections traced the distributed control processes of perception, integration, and articulation in the SOTF's hunt for insurgent targets. All of them manifested an incessant stream of mundane glitches and staffing frictions to be debugged through ever more phone calls, emails, briefings, and new product requirements. The ongoing debugging enabled the information system to implement the SOTF's preferred targeting mission well enough: target packages were produced, triggers were met, missions were executed reliably without catastrophe, and performance metrics were provided to higher headquarters. Many of the raids certainly took a few bad actors off the street, at least for a time; that much seemed apparent from after-action

[79] Regional detention facilities could only hold detainees for fourteen days. If a case could be built against them through recovered evidence or confession (increasingly before Iraqi judges as the legal system matured), then they could be sent to long-term detention and were otherwise released to the local Iraqi Police. Long term detention often had a radicalizing effect on detainees by exposing them to hardened insurgents and by providing them training at "Jihad U." Exposed to U.S. detention and interrogation processes, they could train other insurgents in interrogation-resistance strategies. The experience provided them "street cred" with other insurgents on the outside if they were released. Incarceration was not costless, but the SOTF did not bear these costs directly when it counted interrogation success in terms of long-term detention. The SOTF generally didn't follow up on the detainees it sent.

storyboards. A great deal of administrative work enabled the more celebrated commando exploits.

Yet what does all this activity actually tell us about the SOTF's battlefield effectiveness? First, how well did the SOTF perform its preferred counternetwork mission? Second, how suitable was that performance within the larger counterinsurgency context? These questions are hard to answer because the SOTF manifested not only *interference* friction but also *insulation*. The former emerged through a fragmented system which enabled personnel to inflict negative informational externalities on one another by discarding provenance data, breaking referential integrity, hiding data in labyrinthine warrens, making tacit design decisions, *etc*. The latter emerged through a strong doctrinal consensus for producing and actioning targets amidst a more complicated irregular battlefield. The result of this superposition of frictions was that when targets were poorly constructed, the methodological problems in their construction were rendered invisible as long as the raid went off smoothly. Questions about targeting performance and counterinsurgency context were hard to answer because they could only be addressed within a system which did not readily afford the asking.

7.5.1 Targeting Performance

This section takes for granted the counternetwork theory of victory through attrition of insurgent leadership to assess how well the SOTF implemented this style of targeting.

7.5.1.1 Starting Over vs. Following Through

The SOTF tended to perform each iteration of the targeting cycle as a single phased evolution rather than the cyclic counternetwork feedback loop described in Figure 7-3 at the beginning of this chapter. Once a mission bagged its quarry and filed a storyboard, the Task Unit turned afresh to the next target on its stack rather than pursuing follow-on targets as per the counternetwork ideal. There were always more targeting leads—passed from a Marine unit, named by a HUMINT source, or internal target development—while interrogations and exploitation of material from completed missions might drag on inconclusively for weeks. While the SOTF always had multiple targets at different stages of development, each tended to be independent threads rather than a systematic unraveling of the insurgent fabric.

Starting over constantly rather than following through on leads departs from the counternetwork ideal of working up from insurgent soldiers to lieutenants to high value leaders.

Many SOTF personnel voiced a desire to avoid distraction with "low hanging fruit" and to exercise "operational patience" in order to develop intelligence on the target network. Such patience was more honored in the breech, unfortunately, as the SOTF was better adapted to perform SWAT-type raids rather than drawn out sting-type investigations. As targets became actionable, the Task Units more often than not were tempted to go after them, and once they caught them, they started to look around for the next thing. The failure to connect the articulation phase of one raid into the perception phase of another allowed the underground structure of the insurgency to enjoy dead space while the SOTF was distracted with a series of seemingly disconnected operative cells.

7.5.1.2 The Untouched Underground

Clandestine organizations, under pressure from stronger security forces, adapt to tolerate and replace the loss of their operatives. The most visible insurgents, or "low hanging fruit," are the easiest to find and attack, but for the same reasons, the easiest for the network to regenerate. Clandestine organizations have significant underground command and administrative "tail" with respect to the more visible operative and facilitator "tooth" (a ratio of ten to one in some studies); the former is adapted to survive, while the latter are expendable. Key leaders are less likely to be densely connected to one another because they employ strong operational security discipline and communicate through various cut outs such as couriers, dead drops, codes, and safehouses. The underground is usually far better integrated into and hidden within the local community.[80]

The everyday commerce and behavior—which formed the background of the war and the lifeblood of underground support for the insurgency—was insufficiently understood or mapped by SOTF analysts who focused simply on finding violent leaders. As a result, many of the SOTF's targeting representations revealed small independent cells with fairly unspecific

---

[80] On the structure and importance of organized underground support for insurgent organizations see, *inter alia*: Andrew R. Molnar, Jerry M. Tinker and John D. Lenoir, *Human Factors Considerations of Undergrounds in Insurgencies* (Washington DC: Special Operations Research Office, The American University, 1972); Joe Felter, ed., *Harmony and Disharmony: Exploiting Al-Qaida's Organizational Vulnerabilities* (West Point, NY: Center for Combating Terrorism, 2006); Brian Fishman, ed. *Bombers, Bank Accounts, and Bleedout: Al Qaida's Road In and Out of Iraq* (West Point, NY: Center for Combating Terrorism, 2008); Melvin Gurtov, *Viet Cong Cadres and the Cadre System: A Study of the Main and Local Forces*(Santa Monica, CA: RAND, 1967); Philip Selznick, *The Organizational Weapon: A Study of Bolshevik Strategy and Tactics* (Santa Monica, CA: RAND, 1952); Jones, "Understanding the Form, Function, and Logic"; Benjamin Bahney, Howard J. Shatz, Carroll Ganier, Renny Mcpherson, Barbara Sude, Sara Beth Elson and Ghassan Schbley, *An Economic Analysis of the Financial Records of Al-Qa'Ida in Iraq* (Santa Monica, CA: RAND, 2010)

connections to other insurgent calls. In the haste to "action" these, the SOTF went down numerous "spiderholes" that bottomed out with a single cell, or at most a follow-on mission. When measured in terms of completed missions, dramatic storyboards, and detainees in long-term detention, the operations all seemed successful enough. Yet by leaving the compartmented bureaucratic machinery of the insurgent organization intact, the network retained the ability to replace lost operatives and to survive.[81] Figure 7-9 illustrates how a narrative of SOTF targeting success based on Jackpot storyboards could coexist with a thriving underground network which remained invisible (because of the sampling errors illustrated in Figure 7-6 and because underground support figures appeared to be normal figures in the civilian population).

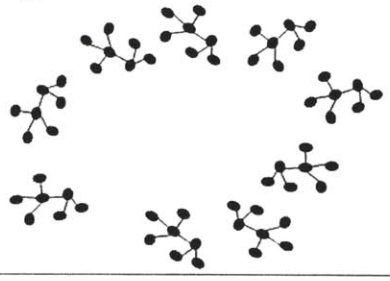
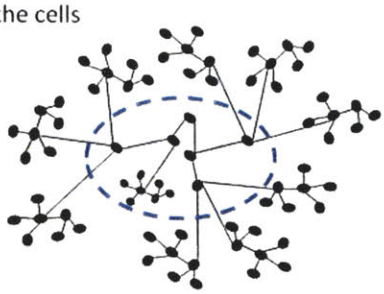
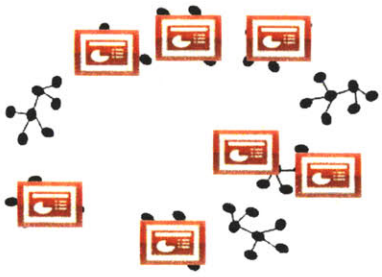
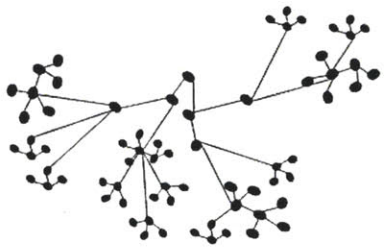
	The SOTF's Representation	The Insurgent Organization
Intelligence collection throughout the rotation	The SOTF finds nine disconnected insurgent cells with actionable intelligence 	The SOTF never finds the links to the underground support and leadership of all the cells 
Operational result after all missions	Seven successful missions (with PowerPoint Storyboards), including one that generated a follow-on mission 	The insurgent organization is able to replace the operatives it loses, and the core remains uncompromised 

Figure 7-9: The SOTF pursues disconnected raids instead of systematic targeting of the underground

It's hard to say whether more analytic attention to interrogation and recovered media—and the follow-on collection such work would prompt—might have revealed deeper connections

[81] Jones, "Understanding the Form, Function, and Logic," 32-44, provides a critique of myopic focus on the visible edges of the network to the neglect of its compartmented administrative core.

to the underground core given the battlefield situation on this rotation. One might argue that there was no underground to find, but that is unlikely given that many of the SOTF's high-value targets were finally killed or captured at a much later date; as of this writing, al-Qaeda continues to demonstrate the ability to stage attacks in Anbar. More likely the underground remained hidden and inaccessible to the SOTF within the social fabric of the province.

7.5.1.3 Data Format Barriers to Self-Assessment

To tease out the real effectiveness of SOTF targeting, beyond the accumulation of storyboards, one would begin with questions like those in Table 7-2, which might be answered by data available in the normal course of mission performance. These questions require the correlation of records about the same entities as they move through the SOTF from perception to articulation. Unfortunately, various parts of the organization tracked similar entities in different ways—through different IT applications, files, features, fields, formats, *etc.*—and only tedious work could tease out references to the same things from these partial perspectives.

Table 7-2: Challenges of targeting effectiveness assessment

Questions about SOTF targeting effectiveness using internally-available data
• Do we target names on our target list, or who have some connection to names on our list? Or do we go after "pop up" targets that we haven't seen before?
• Do we capture the people we target? Do we capture people who weren't targeted? How often do we capture no one at all?
• Do we retarget—plan another mission against the same target—when we miss our targets?
• Do our detainees produce any intelligence about important targets? Does this intelligence lead to follow on targets?
• How many of our detainees go to long term detention?
• Did capturing a particular individual disrupt the insurgency as we expected?
• Did the raid accidentally disrupt something we didn't expect?

To illustrate the problem, I will start with a common targeting ontology that ties everything together and then work backwards to the actual fragmented situation in the SOTF. Figure 7-10 depicts a very simple ontology of entities and relationships involved in the counternetwork targeting cycle ("F3EA"): sources report intelligence, which identifies places, events, and people; correlation of these leads to the designation of some of the people as targets,

which are "actioned" by a mission; a mission yields detainees, which provide more intelligence to feed further iterations. Figure 7-10, which I introduce here only for explanatory convenience, could in principle provide the core of a relational database to rationalize SOTF data management to facilitate structured queries to answer the questions in Table 7-2.

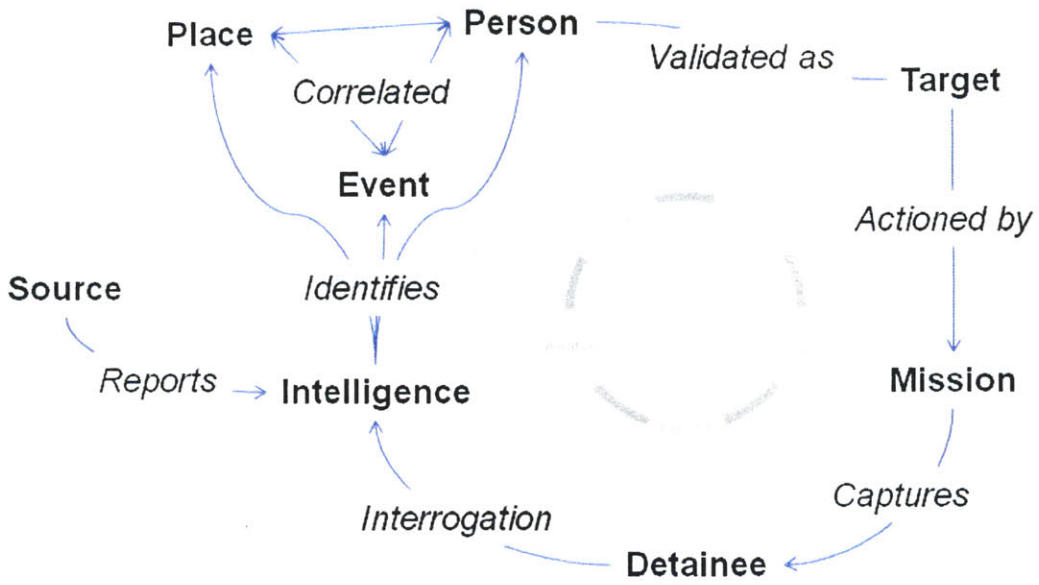


Figure 7-10: Simple targeting ontology with entities (bold) and relationships (italics)

Such a central database did not exist at the SOTF, however. Figure 7-11 depicts various SOTF products with icons for whatever type of media they happened to be (*PowerPoint*, *Excel*, *Word*, webpage, *etc.*). Figure 7-11 shows how different products in use at the SOTF reference the same ontological types in our data model. The relationships among entities include: TIPs are one-to-one for each target; target lists are one-to-many with targets; intel products are many-to-many with people, places, and events; *etc.* Figure 7-11 is still an ideal depiction because it shows all the products together, already mapped to the various ontological entities they represent. In the real SOTF there was no common data model or ontology. I introduced it simply to show how different products pick out roughly the same types of real-world entities. In reality, these products all resided in different data warrens, and they were created and managed by different parts of the organization to facilitate the performance of their narrow part of the mission.

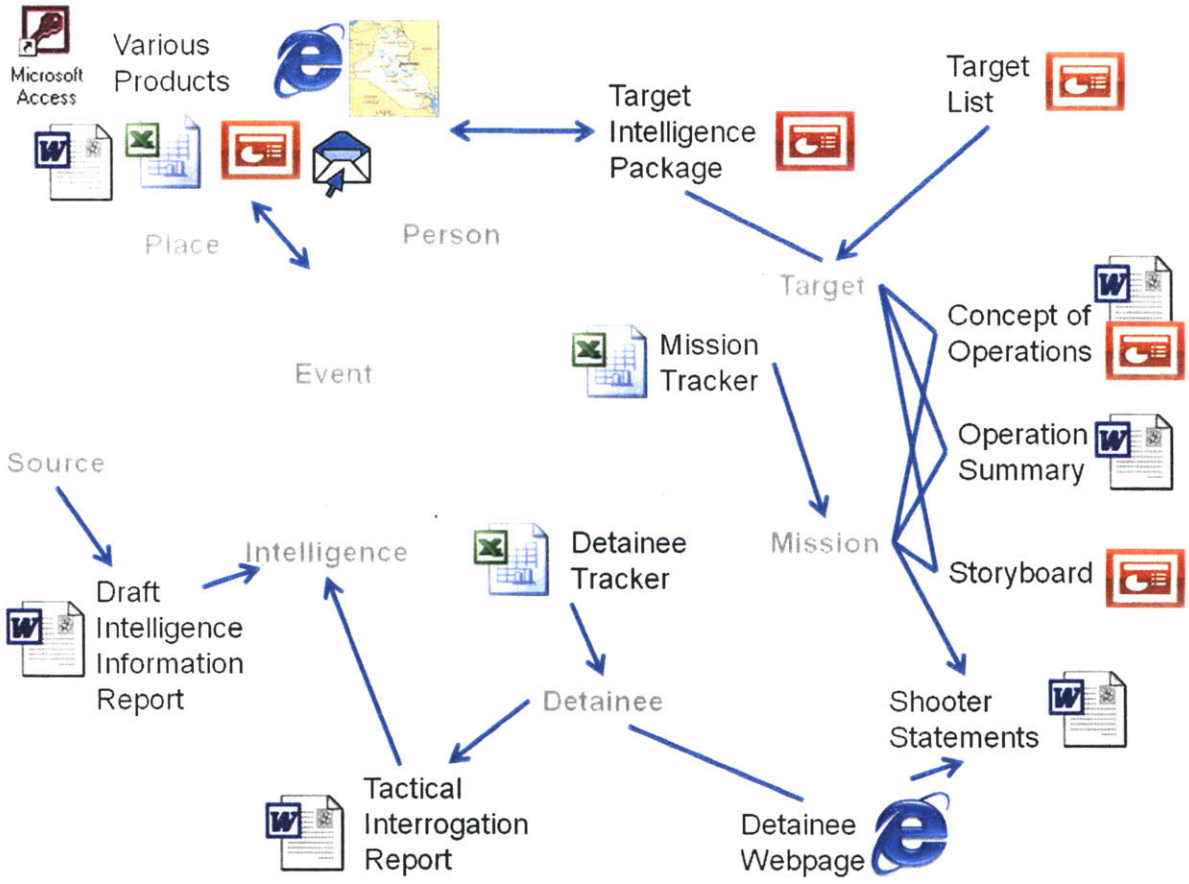


Figure 7-11: Arrows show the relation between the information product and the ontological concept

In the actual SOTF, the discovery of these entities, their content, and their ontological relationship required a spelunking trip through SOTF data stores, illustrated in Figure 7-12. Task Units generated most of the products (TIP, CONOP, OPSUM, TIR, DIIR) and emailed them to one of the staff sections in the SOTF HQ, while a few (Mission and Detainee trackers) were headquarters products. All of them supported narrowly scoped parts of the process for specific actors working on pushing through individual missions, so these products were saved in different share drive folder hierarchies. While all of the products touched on people, they did so at different stages in the process and touched them in different ways (as suspects, targets, or detainees). The traces that they left in the system were not commensurable. With little configuration control across the enterprise, the format of these products was out of sync, and jurisdictional boundaries partitioned access to some of them.

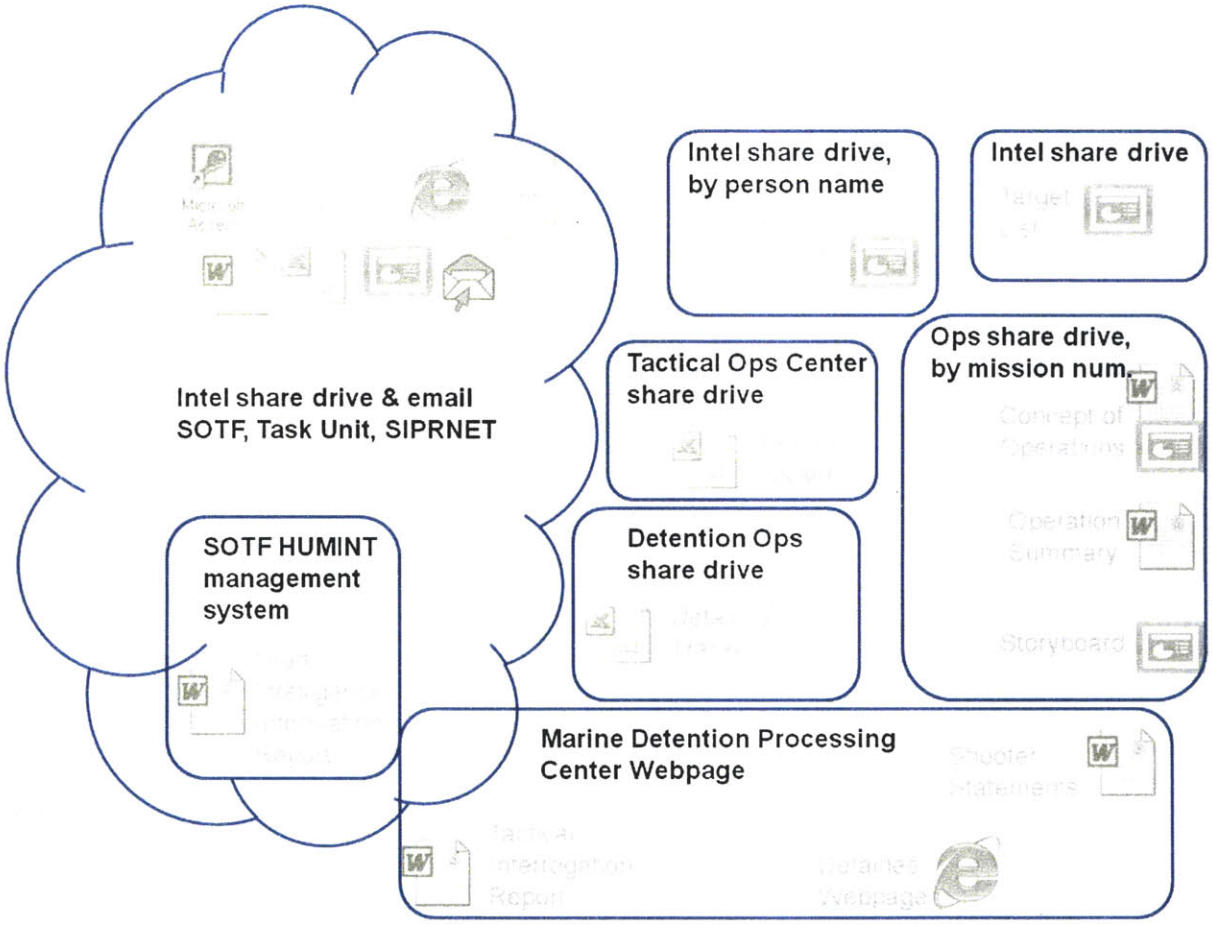


Figure 7-12: Location of representations on organizational file servers

All of the products in Figure 7-12 evolved to support a series of unrelated but routine targeting drills. They did not evolve to ask questions about the aggregate. The organization's representational infrastructure emerged in a discombobulated way through a history of actual use, and this imposed costs on reordering it to support new kinds of questions. In order to ask questions across these differently-situated products, you had to go through the share drive and through the halls of the SOTF to understand these products and their relationships. Thus you had to first obtain access to them and then figure out how data owners of each product updated data and structured data elements. In opening up and comparing individual files, you most likely would make working copies of them to facilitate compilation in a new fusion product like a spreadsheet. The only way to tell whether two different products referred to the same entity would be by matching up common data elements across products. Created for human reading and not machine comparison, data elements were formatted differently, with varying Arabic

transliterations, so this matching required much manual review and "data massaging." Figure 7-13 shows relationships among different SOTF products without the useful crutch of the common ontology in Figure 7-11; that is, Figure 7-13 shows the actual correlations someone would have to make to ask cross-cutting questions.

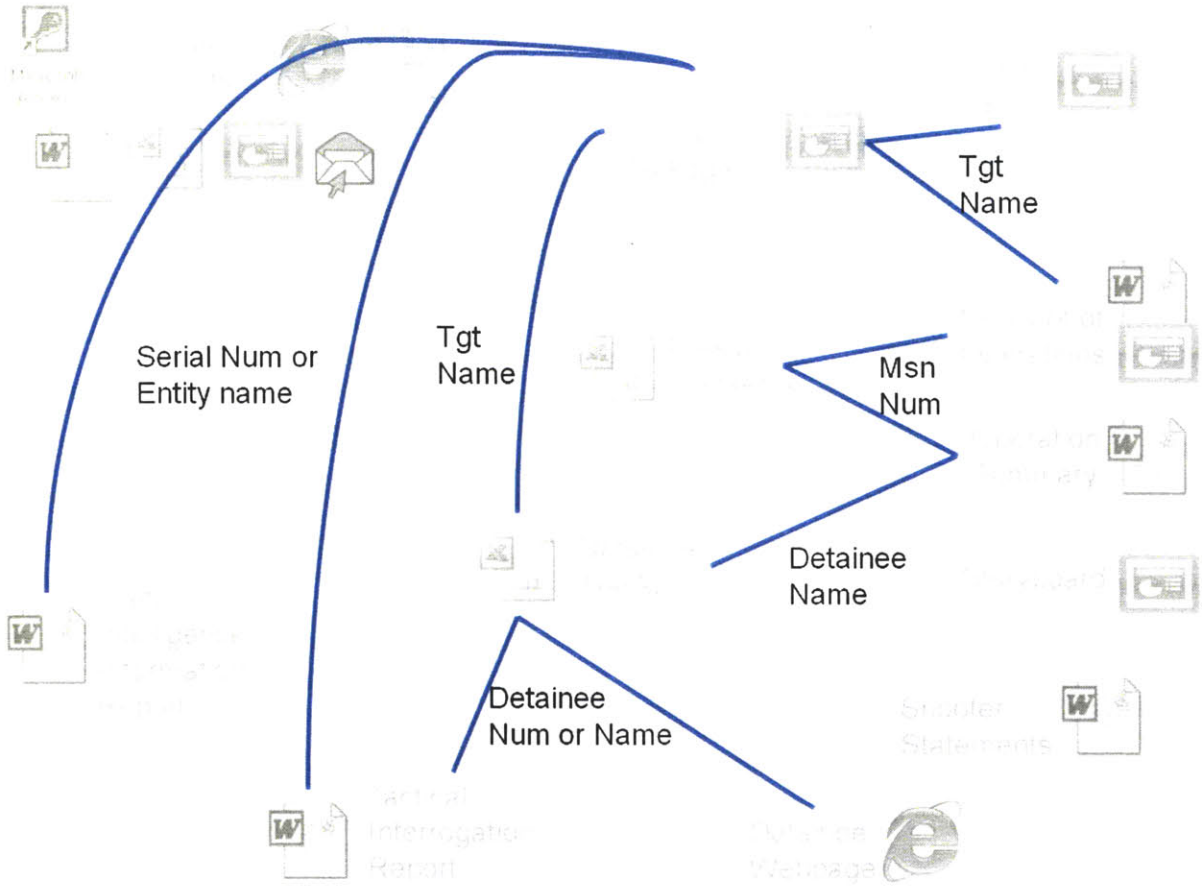


Figure 7-13: Shared data elements linking representations together

To query this distributed data, you had to compare different files controlled by different staff members who were not necessarily interested in answering boundary-spanning questions. For example, if you wanted to find out if a mission on the mission tracker spreadsheet went after a target on the target list, you would have to first get the mission number, then go to the folder by that number and open the CONOP document. You would have to compare the target name on this to the *PowerPoint* target list (or the target list of each Task Unit). If the name did not appear on the list, you would have to go to *PowerPoint* target folder with the target's name as the filename, and look through it to see if the mission's target at least had a relationship to someone

on the list. Two simple modifications would have made this comparison much easier: (1) keep the target list as a spreadsheet instead of a *PowerPoint* slide, and (2) include the target name on the mission tracking spreadsheet. This small modification would have simplified the calculation of answers about a single target as well as about how many missions in total went after names on the target list.[82] Yet no one person owned these products and simultaneously understood their details. The officer in charge of keeping the target list needed to brief it during weekly staff meetings, so he stored the data as a *PowerPoint* slide. His list was formatted for viewing rather than data processing. This officer perceived storing a spreadsheet to be just extra work on behalf of another staff member with no clear intelligence value.[83] The tactical operations center (TOC) was not in the habit of recording the target name in the mission tracking spreadsheet, and it was a regular effort to persuade them to do so. The TOC used the mission tracking spreadsheet as a simple event log for the different phases of a mission, rather than to facilitate performance assessment across missions.[84]

The inverse problems of figuring out whether a particular person had ever been targeted in a mission, or who were the people recovered by a mission, were even harder. The mission

---

[82] I went through this tedious exercise and found that a surprisingly small percentage—well less than a quarter—of raids actually targeted someone on a target list. Thus targets were at best associated with someone on a target list (or associates of associates) or they were pop-up targets.

[83] A spreadsheet—or better, database—of targets would have opened up possibilities of quickly linking targets to missions, and intelligence reports to target, providing a view of organizational performance across seams. Briefing slides could even have been auto-generated. Yet, unfamiliar with the technical possibilities, and needing to have briefing slides with fancy formatting and pictures, the idea of rational data-management ideas was rejected as excess work without obvious benefit.

[84] The following story illustrates the sort of formatting headaches that prevent aggregation across different local jurisdictions. I often tried to use a spreadsheet to compute summary statistics across all SOTF missions. Numeric fields like time had omitted digits, the letter "O" for the number "0" or vice versa, padded spaces before text, variant spellings, synonyms, omitted fields, *etc.* These errors only jumped out when I attempted to calculate totals on categories, or join the data to other data. Getting these errors corrected was a delicate matter with the TOC chief who insisted that "there are no mistakes in my spreadsheet." "Mistakes" for him meant omitted missions or an incorrect mission status, not something trivial like commensurability. Recognizing the centrality of the mission tracker for linking together a lot of information that came through at mission run time, I prevailed on the operations officer to insist to the TOC that the mission tracker be expanded to include many other descriptive fields like the name of the targeted person, detainees captured, and the result of the mission. We added these fields to the right of the existing ones in the spreadsheet so as not to disturb the layout that was familiar to the TOC watch. The TOC did start populating and cleaning up these fields after some cajoling. To my surprise, however, I walked in one evening and found that they were actually keeping two separate versions of the mission tracker, one with the expanded field list, and one with the original format! They said the duplication was easier for them to manage, so they could display the original version on a projector and assign someone else to populate my expanded data. I started to get the data I needed so I didn't argue with them, even though the left side of both spreadsheets appeared visually identical.

products (CONOP, OPSUM, Storyboard) were saved on the share drive in folders by the mission number, which were assigned chronologically without regard to the target. Many missions might not recover the named target, but would still return with "Persons Under Control" (PUCs) who had behaved belligerently or suspiciously on the objective (or, as was frequent earlier in the war, just happened to be males of military age); such PUCs were otherwise unknown quantities for the interrogator to evaluate. Thus a mission which was not a "Jackpot" might still not be a "Dry Hole" if non-target PUCs had been captured. The mission tracker spreadsheet listed neither target nor PUC names. A separate detainee tracker spreadsheet, managed by the Detainee Operations officer, associated detainee names and mission numbers. The names were be rendered with transliterations given by interpreters at the detention facility, which might not match target names exactly if the PUC actually was a target, and wouldn't match at all if he wasn't.[85]

These irritating problems often came up when questions spanned two different pools of data with slightly different ontologies rooted in different tasks. Aggregate questions couldn't be asked easily if data storage did not afford recombination. Aggregate answers, if they were requested at all, required manpower intensive "data scrubs" requiring the construction of parallel, static, one-time representations, not queries that could be run at any time on an active data store. Repeat questions required repeat scrubs in order to implement a very slow query over this very noisy database.[86] This example has hopefully conveyed some of the decidedly unromantic daily experience of staff personnel in an IT-intensive environment.

---

[85] To assess whether detainees were providing intelligence for new targets, you had to associate interrogation reports to detainees and then to follow on target development. Detainee numbers on interrogation report would have to be correlated with the number on the detainee tracker, which might changed as detainee custody shifted among detention facilities. Then the entities named in the reports would have to be correlated with subsequent TIPs, which Task Units might not have shared with the SOTF to avoid headquarters scrutiny. It was difficult to assess the value of detainees simply within the context of supporting the F3EA cycle (i.e., whether they provided targetable intelligence).

[86] Another option, requiring specialized technical savvy and the creation of supplemental representations, would be to transform the data from its local stores by writing scripts to parse and recode it. Doing so would require setting up supplementary data stores, such as one that might add additional fields to the mission tracker, or bind it to the detainee tracker. Such feats of data juggling introduced great configuration management problems for the lone virtuoso, struggling to get the latest data incorporated into comprehensive representations with a minimum of manual reformatting. Expert data-massage skills were in short supply, however, and were, moreover, undervalued when run-of-the-mill email and *PowerPoint* skills allowed most staff officers to get by.

When an enterprise problem is seen holistically, then these various problems seem trivial and the normalization of data seems like a solvable engineering problem. It might be solved, that is, *if* one has the persuasive influence, the organizational authority, the data access, the technical skills, the time and the manpower to render this mass of data commensurable. That is, there is actually a political or leadership problem in the midst of the technical data management problem. Rather than expending the effort to solve either, staffs tended to tax subordinates with new reporting requirements in specific formats, simply outsourcing the manual load of computing aggregation. Unable to combine technical skills with cooperation across staff-sections to find out what answers might exist in data already within the headquarters, staff officers found it more expedient to exploit hierarchical command relationships with subordinate units to get the information work done. *The SOTF didn't know what it knew*, in effect, because personnel didn't (or couldn't) ask questions that lacked socially-structured information channels for the answers.

The reason that these tedious administrative details matter is that if an organization can't compare across data pools, then it can't really assess how well it's doing. The data needed to assess counternetwork performance was fragmented across SOTF data stores and formats. Given barriers to answering questions of performance, they tended not to be asked. The SOTF's information system canalized the organization into the repeated performance of one-off raids. IT itself does not have a targeting bias, for it is the means to represent any version of reality, but the way in which it was employed tended to canalize perception into a targeting worldview. Evaluative feedback is always a demanding, information-intensive problem with a heavy cognitive/computational load. Yet the SOTF's supply-side information-processing capabilities were not up to the task given the SEAL community's disinterest in conscientious, competent, information work in comparison to commando proficiency. The SOTF improvised a jumble of *ad hoc* representational processes—abetted by powerful and flexible IT in the hands of personnel with little interest in learning how to get the most out of them—to execute the types of operation that it most preferred to do. The organization's tangled information architecture helped to amplify its own biases.

7.5.2 Counterinsurgency Performance

Information friction biased SOTF attention toward available "low hanging fruit" and impeded self-assessment. As a result it did not perform truly cyclic counternetwork operations

and thereby contributed to dead space wherein the underground core of the insurgency could plan and regenerate. Beyond whether counternetwork targeting was implemented skillfully or not, however, there are further questions about the effect of special operations raids on the broader dynamics of civil war. That is, how might the SOTF assess whether its problem wasn't just counternetwork performance, but the whole premise of victory through counternetwork attrition? Questions like those in Table 7-3 were difficult to ask given the information in and analytical focus of the SOTF. The organization's relative autonomy and doctrinal consensus insulated it from having to ask them seriously.

Table 7-3: Challenges of counterinsurgency effectiveness assessment

Assessing SOTF effectiveness within larger counterinsurgency mission
• What is the real military and political balance of power on the battlefield?
• How is the insurgent underground sustained politically, economically, and ideologically? What is the regenerative capacity of the various insurgencies we face?
• Are counternetwork operations a complement to or inhibitor of "hearts and minds" counterinsurgency?
• What are the second-order effects of counternetwork raids? Do targeting errors and violent raids foment resentment in the local population, generate insurgent recruits, undermine development projects, or compromise the legitimacy of Iraqi Security Forces?
• Which type of targeting error is more costly in the long term: false positives which hit unimportant insurgents or innocent civilians, or false negatives which leave dead space for insurgents and corrupt elites?
• Are there lost opportunities for overt or clandestine intelligence collection that might contribute to a better understanding of the systemic dynamics of civil war? How can we better learn about what is really going on and educate our forces?
• Are there indirect methods—through civil affairs, tribal engagement, or information operations—to influence local allies and adversaries?
• Are our operations here helping to "work us out of a job" or are we merely "playing whack-a-mole" and "mowing the grass" with the endless targeting of a regenerative foe?

7.5.2.1 Full-Spectrum Counterinsurgency

It is beyond my scope to discuss counterinsurgency alternatives to counternetwork operations in much detail. The proportion of discussion of counternetwork to counterinsurgency operations in this chapter roughly parallels the SOTF's allocation of attention and resources on

the deployment. I have intentionally left out this larger context until now in order to convey a sense of the insulation of the SOTF's world.

Social science understanding of clandestine networks and their interaction with a developing economy is not mature (to say the least) and will remain an active area of research for some time. Chapter 5 discussed how the diminution of violence in Anbar is poorly explained by the counterinsurgency field manual written for Iraq. It is fair to say that, despite the profusion of counterinsurgency literature in the last few years, there is still an uneven understanding of what military and political methods are and aren't effective for suppressing rebellion. Intellectual hubris is a major challenge in irregular war. The first cause of information friction—the external instability of a dirty battlefield—has a pronounced effect in this problem.

During the deployment I found Roger Petersen's *Resistance and Rebellion* particularly useful and relevant to the situation in Anbar.[87] Peterson argues that different segments of a population can be triggered to participate in different levels of rebellion: unorganized opposition to the government, locally organized provision of intelligence and material support for insurgency, and mobile guerrilla combat units. Peterson describes triggering and sustaining mechanisms at each level.[88] A natural extrapolation is that counterinsurgency should endeavor to inhibit these mechanisms and to take proactive measures to trigger shifts in the opposite direction.[89]

---

[87] Roger D. Petersen, *Resistance and Rebellion: Lessons From Eastern Europe* (New York, NY: Cambridge University Press, 2001). A close second for practical utility among academic works on civil war was Stathis N. Kalyvas, *The Logic of Violence in Civil War* (Cambridge University Press, 2006).

[88] Petersen, pp. 32-79, focuses on the transitions from 0 to -1 and -1/0 to -2 in Figure 7-14, with minimal discussion of transitions to -3. I supplement his mechanisms with the administrative "organizational weapon" that enables the combatant core of most insurgencies, and which sharply distinguished the planning, fighting, and survival capacity of al Qaeda in Iraq (AQI) from the traditional/charismatic leadership of the tribes. I have also supplemented Petersen's theory with material incentives for participation (fees, trafficking rents, pensions, health care, life insurance, *etc.*), which apparently were not prominent in Petersen's Lithuania case. Material incentives certainly mattered in Anbar for paying for intelligence, IED emplacement, and the tribal-AQI dispute over smuggling lanes. On AQI rational vs. tribal traditional/charismatic leadership in Anbar see Austin Long, "Strategies of Tribal Engagement: From the Awakening to Iraqi Statehood," paper presented at International Studies Association annual conference, New York, NY, 15 February 2009.

[89] Counterinsurgency doctrine has been derived inductively, more or less, from practitioner memoirs of what worked in actual campaigns, usually at fairly local levels. It rarely has been connected to social science theory of the causes and conduct of civil war. The counterinsurgency measures listed in Figure 7-14 are consistent with the "population centric" counterinsurgency literature, but they are linked explicitly to theoretical explanations for rebellion. That is, counterinsurgency doctrine has collected a lot of intuitions about approaches and tactics that have worked, but it hasn't been able to explain why or under what conditions they work.

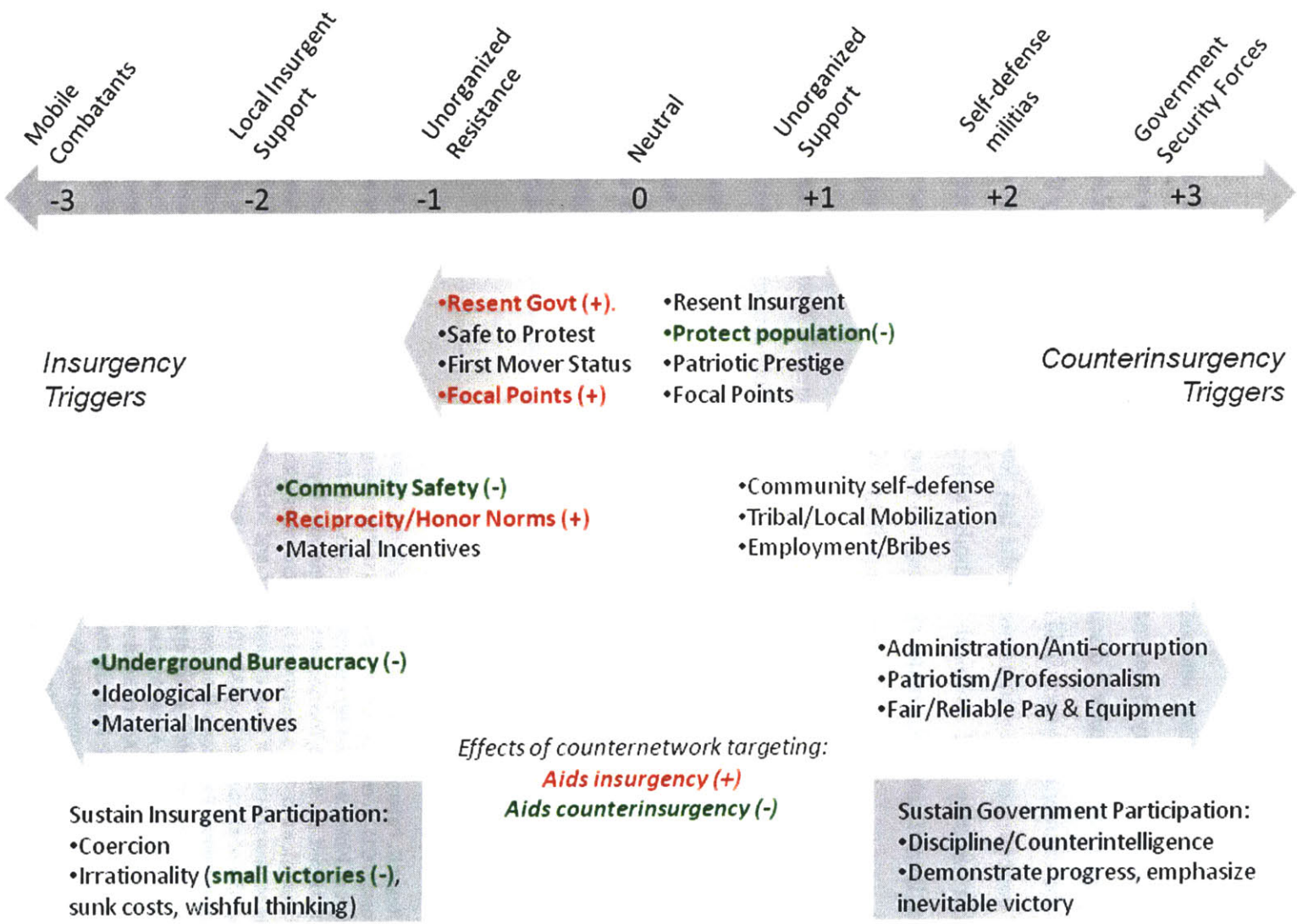


Figure 7-14: Triggering, counter-triggering, and sustaining mechanisms for (counter)insurgency

An appendix to this dissertation describes the ideas in Figure 7-14 in more depth and discusses differences in conventional and special operations forces implementation of them.[90] The key point for this discussion is that counternetwork targeting can both assist the inhibiting mechanisms as well as exacerbate the insurgency triggers. Counternetwork targeting can inhibit insurgency by altering local safety calculations for insurgent participation and by eroding the bureaucratic administration of an insurgent organization. Yet counternetwork targeting errors and excessive "kinetic" violence can also amplify Petersen's triggering mechanisms for rebellion. Poor coordination with the "non-kinetic" negotiation, development, and marketing efforts of other counterinsurgents can also undermine the countertriggers. "Kinetic" abatement of the insurgency is thus only a small part of the overall suite of tools to be employed. It completely ignores the alliance-making, patronage (bribery) payments, and amnesty deals which figure prominently in the resolution of many counterinsurgency campaigns.[91] To the degree that a full-spectrum approach to counterinsurgency was implemented in Anbar, the Marines rather than special operations deserve most of the credit.

Empirical investigation of these claims—as well as testing of all the various mechanisms of counterinsurgency proposed in the literature—remain open problems in civil war research. I mention them here only to point out the interactive complexity and broader counterinsurgency context of the SOTF's targeting operations; these considerations introduce reasonable questions about the efficacy and counterproductive effects of counternetwork targeting. Suffice it to say, it was difficult to get much traction on such questions within the SOTF's information system.

7.5.2.2 Measures of Effectiveness

The SOTF tended to measure its own performance more than its effectiveness in the broader environment: success was in the raid itself and a dramatic storyboard. Measures of effectiveness are notoriously difficult to define for counterinsurgency, owing in part to immature social scientific understanding of the phenomenon. Task Units could not really state the intended effect of each particular mission beyond vague nostrums like "disrupt the insurgency."

---

[90] See Appendix: A Theory of SOF Full-Spectrum Counterinsurgency

[91] Many historical rebellions have certainly been crushed with brutal military force and little attention to "hearts and minds." The diversity in the conduct and outcome of civil war calls for the development of theoretical conditions for the broad generalizations prevalent throughout counterinsurgency doctrine. On false dichotomies and bad historical analogies in counterinsurgency see Kelly M. Greenhill and Paul Staniland, "Ten Ways to Lose At Counterinsurgency," *Civil Wars* vol. 9, no. 4 (2007): 402-419

Even if the expected effects of missions could have been clearly specified, SOTF combat assessment would then have to measure the effects of the action. Such measurement would have to redirect the intelligence resources used to identify and track targets, especially HUMINT, to illuminate interactions within the society. Sources would have to be developed to inform on tribal politics and economic transactions, and analysts would have to be able to map the broader social milieu on which the underground was parasitic. They would need theories to guide their work as well as better societal data to assess. Such work might not ever yield future targets.

Furthermore, the SOTF was only one small organization within a much larger Marine effort in Anbar, so it would be complicated to tease out the marginal effectiveness of specific SOTF raids compared to other American and Iraqi efforts. The measurement of macro political and economic variables in the province, let alone the micro-activity of tribal actors, was hard enough; drawing causal links to SOTF activity was another thing entirely. Little wonder the SOTF stuck to a simpler storyboard-based narrative of effectiveness. There was little dedicated analytical effort or focused collection for either retrospective assessment of targeting missions or causal connection of commando raids to the broader society. The SOTF instead just looked for new targets and measured its own behavior in raiding them. That is, concrete measures of targeting behavior were substituted for ambiguous measures of counterinsurgency effectiveness.

7.5.2.3 Data Content Barriers to Self-Assessment

In contrast to the institutionalized channels which shaped target-relevant information in SOTF perception, the information needed to assess the political context of military operations was even more fragmented. Whereas intelligence databases, reporting channels, and targeting shops existed to map insurgent networks and construct target folders, there was little comparable analytic infrastructure for political-economic intelligence.[92] Relevant data could be found not only through intelligence channels, but also through patrol reports, civil affairs reports, State Department diplomatic reporting, and media sources. The consolidation of this data was haphazard, and it all had quite different formats and intended audiences. This type of information was usually of little actionable targeting value, yet it was invaluable for understanding Anbari society (Figure 7-15 shows Sheikh Mishan al-Jumayli, in the town of Karmah on the outskirts of Fallujah, explaining a genealogical chart of his tribe, tracing its

[92] Political-economic analysis cells in various intelligence centers existed but were dwarfed in comparison to targeting cells.

ancestry back to the Prophet Muhammad.). Chapter 5 described how in Anbar province, local engagement through civil affairs patronage projects and alliances for intelligence and manpower ultimately proved more important than unilateral combat for defeating al-Qaeda in Iraq.

Figure 7-15: Sheikh Mishan al-Jumayli explains his tribe's genealogy (Author's photo)

While killing and capturing insurgents may have been necessary for protecting the population and for providing disincentives for participation in insurgency, such activity needed to be integrated with the Marines' more important "non-kinetic" efforts to reassure the tribes, improve economic development, and enhance the rule of law. Without systematic combat assessment of targeting in its societal context, "F3EA" became an endless do-loop that neglected alternative persuasion and engagement options as well as local allergic reactions to violent raids that could undermine the entire enterprise. Targeting errors with obvious and immediate effect—friendly casualties or spectacular collateral damage—were matters of great concern to SOTF officers, as they were accompanied by clear signals. However, the signals of targeting

errors with more latent effects were lost in the pace of operations, which bounded ever forward. SEAL culture hardly encouraged the tedious forensic work on past targets which would have been required to detect these more subtle signals.

The operative part of an insurgency is just the tip of the iceberg. Beneath lays a clandestine underground network intertwined with local communities. As the SOTF picked away at visible ice, it had trouble seeing whether or not they were all part of the same underwater berg. Alternative approaches to counterinsurgency that might instead try to melt the iceberg from below, rather than chip it away from above, were not readily perceived through the lens of the SOTF's target-focused information systems.

7.5.3 High Information Friction with Modern IT

I must emphasize in closing the SOTF's use of IT to reinforce a targeting worldview should not be misconstrued for sinister intent. While I did encounter some instances of uncorrected incompetence, gross parochialism, or bloodthirsty hubris, most personnel most of the time worked hard to do the right thing: to get the bad guys and to protect the good guys. Intelligence analysts and staff officers toiled sleeplessly to build information products to support the mission. Operators courageously took personal risks and, by and large, conducted themselves professionally in the field to capture some dangerous characters. They helped their Iraqi partners to improve their tactical soldiering skills and judgment. The reader should see no malign conspiracy in the SOTF's target-centric view of the world, or in the difficulties it encountered in verifying whether its targets and detainees really were nefarious. It was a war, after all, and the SOTF's job was—in part—to hunt the enemy.

The tragedy is that this earnest performance was at best difficult to measure and at worst counterproductive. Targeting is a necessary task in counterinsurgency; however, it is not the only task. The prior organizational preferences which the SOTF brought, the *ad hoc* organizational architecture it cobbled together, and the way it manipulated flexible IT, all systemically reinforced a target-seeking worldview which filtered out information on slow-burning targeting errors. The SOTF's representational architecture served as a filter for designating and tracking targets. Even in that endeavor it was a noisy channel.

While SEALs often repeated the maxim that "we can't kill our way out of here," they nevertheless were eager to find ways to do so. With all the noise in SOTF information systems, one might reasonably question the "quiet professional" moniker. Given the insulation of targeting within the broader counterinsurgency mission, one might also question the popular image of special operators as versatile specialists in unconventional warfare who accomplish their work by, with, and through the indigenous population.[93] The SOTF was given—and it advertised to visitors—a full-spectrum mission to professionalize Iraqi security forces, conduct civil affairs with local tribes, and to combat the insurgency. Yet in practice it reluctantly carried out, haphazardly dabbled with, and enthusiastically embraced these respective missions. The outcome was an ambiguous episode in a protracted attritional campaign.

Table 7-4 lists the distributed cognition manifestations of information friction, with a couple of examples of each drawn from the many more discussed above. As in the phenomenological and prosthetic manifestations of friction summarized in Chapter 6, there is not a clean coding of low and high friction, but instances of both and wavering between them. This is especially the case given a superposition of interference and insulation. Interference is palpably high friction amidst uncoordinated systems, whereas insulation involves some locally low friction which is systemically inappropriate for the environment. SOTF agreement on the desirability of targeting doctrine and optimization of information systems to support its performance allowed for pools of low friction in the SOTF. These can be considered minor RMA successes. Yet the insulation of the whole system acutely qualifies such success. Clearly the context of employment matters tremendously, as the SOTF's usage of powerful, networked IT also supported performance outcomes at odds with RMA expectations of rapid, decisive, low-cost victory.

---

[93] Army Special Forces rather than Navy SEALs have historically personified the unconventional warfare approach rather than the commando direction action and special reconnaissance emphasis of the latter (even though SEALs have long been involved in the Foreign Internal Defense mission of training security forces in the developing world). However, as discussed in Chapter 5, there has been a pronounced upward harmonization of U.S. special operations forces toward the direct action *modus operandi* of the national special mission units. Furthermore, SOCOM increasingly treats SEAL Platoons and SF Teams as interchangeable Joint parts on irregular battlefields. The net result is that both Army and Navy special operations are supposed to be able to do indirect action missions, but both have strong preferences for direct action. Thus while policymakers may believe they are getting full-spectrum unconventional warriors for their special operations dollars, they will more and more be buying commandos, whether colored green or blue.

Table 7-4: Some manifestations of information friction in SOTF targeting

	Low Information Friction	High Information Friction
Distributed Cognition *(Systemic qualities of human-machines implementation of control cycles)*		
IF11. Computational Goals	*Defined/shared* Counternetwork targeting	*Ambiguous/controversial* "non-kinetic" counterinsurgency
IF12. Implementation	*Efficient* Air mobility, full mission profile, ISR tactical coordination	*Ends-means misalignment* Noisy targeting processes & counterinsurgency mismatch
IF13. Routine Performance	*Heedful interrelating* Operational safety, SEAL tactical communication	*Mindless execution* On to the next target, uneven analytical savvy
IF14. Command and Control Doctrine	*Orients practitioners to bureaucratic format* F3EA as a targeting ideal	*Simplistic omission of messy realities* F3EA amidst counterinsurgency
Perception *(Transduction of environmental situations into detached symbols)*		
IF15. Cascades of inscription	*Constrained transformation* ISR control, SIGINT systems	*Corrupted, noisy* political-economic data, language barrier, ISR data
IF16. Referential integrity	*Preserved* Prowords, much reporting	*Equivocal* HUMINT control & reporting
IF17. Provenance	*Recorded & reliable* Embedded files in target folder	*Unknown* Sanitization, cut-and-paste, DIIR references, local databases
Integration *(Combines incoming information with information in memory)*		
IF18. Centers of calculation	*Panoptic "common operational picture"* Blue Force Tracker	*Illegible/fragmented or insular/oblivious* Battle tracking products, digital IT tools (Chapter 6)
IF19. Abstractions	*Dependable "black boxes"* logistics, network diagrams of infrastructure	*"Leaky" implementation* Social network diagrams, target folders
IF20. Decision-making	*Efficient* CONOP, Target folder	*Sclerotic or neurotic* Counternetwork feedback, political-economic data, "kill tv," strategy & guidance *PowerPoints*
IF21. Mobilization	*Mission functional* Mission planning & administration, tactical intel graphics, target lists, target folders	*Political rhetorical* Selling targets, CONOP manipulation, target lists, storyboard trophies, "confidence operations"
Articulation *(Transduction of symbols into action in the environment)*		
IF22. Dead reckoning to contact	*Reliable reconnection* Full mission profile planning & execution, PUC	*Unpredictable collision or unable to connect* Dry holes, collateral damage, ambush
IF23. Feedback	*Triangulation & self-correction*	*Allow enemy "dead space"*

	ISR overwatch	"spiderholes" and the administrative underground
IF24. Closure	*Close on entities of concern (enterprise integration)* Jackpot	*Hung open or premature closure (interference and insulation)* Target error (false +/-), indirect action opportunity cost

7.5.4 A Stiletto is not a Swiss Army Knife

In the final analysis, U.S. special operations forces have developed a potent "organizational weapon." The upshot of internal consensus—doctrinal cohesion and control over the protocols of representation—is a reduction of information friction in the appropriate circumstances. The SOTF's most reliable information processes supported core commando tasks as well as routinized operations like air mobility and headquarters reporting. In terms of the phases of control, the SOTF's articulation phase was more stable than either perception or integration, with the articulation of raids driving the whole cycle. The SOTF could be an effective lethal tool given complementary objectives. Yet to the degree that the Anbari environment called for a more nuanced and indirect approach to counterinsurgency, then the SOTF's stable performances were insulated from it. Because special operations forces have such strong cultural preferences, it can be dangerous to increase their autonomy, secrecy, and resourcing in an environment which is misaligned with those preferences.

Irregular war is a complex business where the bulk of the effort should be focused on intelligence gathering and political negotiation, awaiting for opportunities to develop rather than trying to offensively force them. Commandos and their information-processing entourage are good at only a narrow part of this mission. U.S. special operations provide a stiletto, good for dispatching rivals in a dark alley, but not a multitool Swiss Army Knife, good for opening cans of food and mending barbed wire. Policymakers should understand the difference before flashing any steel.

Chapter 8: The Battle of Britain

This dissertation has developed a theory of information friction, which is the struggle to coordinate information technology (IT) and political processes with the structure of the environment in the midst of wartime operations. While militaries usually embrace IT in an attempt to boost performance, practical usage can also exacerbate organizational pathologies. The theory draws on the sociology of technology literature and is grounded in a participant-observer study of military IT usage in a U.S. special operations task force (SOTF) in Iraq in 2007-2008. A reasonable question is whether these ideas apply outside of the odd little terrarium that was Anbar Province. Indeed they do, as this chapter will demonstrate with the information system that fought and won the Battle of Britain.

8.1 Case Selection and Methodology

The 1940 battle is widely recognized as a critical episode in the Second World War, for it showed that Nazi offensives could be broken and enabled the British to stay in the fight. Only slightly less well-appreciated is its influence on command and control (C2) and IT in general well beyond the war. Fighter Command's innovative air defense system established many of the terms of reference and basic processes for more sophisticated air defense and airspace control systems to come later (early warning, common air picture, identification friend or foe, aircraft vectoring, *etc.*). Its legacy includes the American Cold War era Semi-Automatic Ground Environment (SAGE), which spurred the development of several critical digital technologies like magnetic memory and pointing devices.[1] Both air defense and IT were in their formative years in Fighter Command, and it turned out to be a fortuitous combination.

Fighter Command has been described as "the classic modern C2 success story, the example usually cited when the topic is the force multiplier effect of capable C2."[2] Most historians, likewise, credit the integrated *system*—above and beyond radar or fighter technology

[1] Kent C. Redmond and Thomas M. Smith, *From Whirlwind to MITRE: the R&D Story of the SAGE Air Defense Computer* (Cambridge, MA: MIT Press, 2000); Thomas P. Hughes, *Rescuing Prometheus: Four Monumental Projects That Changed the Modern World* (New York, NY: Vintage, 1998)

[2] Thomas P. Coakley, *Command and Control for War and Peace* (Washington DC: National Defense University Press, 1992), 29

alone—as an essential factor for explaining the battle's outcome.[3] Information friction theory must, therefore, be able to explain this important success story if the theory is worth its salt.[4]

Chapter 4 described three conditions that are necessary for IT usage to deliver the sort of "situational awareness" and responsive operations expected in "revolution in military affairs" (RMA) doctrine. *External stability* ("third image" strategic structure) is the ability, given the technical state of the art, to establish connections with operationally-meaningful features on the battlefield: the world must be knowable in principle. *Internal consensus* ("second image" bureaucratic politics) is rough agreement among actors with a stake in the information problem about how to mobilize bureaucratic and technical resources to solve it: the organization must agree on how to know the world. These two conditions inevitably weaken in war, and thus information friction makes it hard for the information system to close control loops on the enemy (or allies). *Expedient adaptation* ("first image" individual behavior) is the reconfiguration of information systems on the fly by locally-situated actors who can exploit low boundaries between technical expertise and operational needs. The adoption of more complex IT makes the first two conditions harder to meet and thus places greater reliance on the third.

In the interwar years the British developed novel ways to employ cutting-edge IT of the day (radio, radar, analog computers, *etc.*) for aircraft detection and communication. Given general scholarly agreement about the positive contribution of these IT networks to the military outcome in 1940, we had better see all three conditions met, or else we have to reject the theory. Such a test requires detailed examination of the context and operation of the perception, integration, and articulation phases of organizational control. Fortunately, the Battle of Britain is one of the most thoroughly documented episodes of the Second World War, which provides the

---

[3] The literature on the Battle of Britain is enormous. I have relied heavily on the following: Derek Wood and Derek Dempster, *The Narrow Margin: The Battle of Britain and the Rise of Air Power, 1930-1940* (Washington, DC: Smithsonian Institution Press, 1990); David Zimmerman, *Britain's Shield: Radar and the Defeat of the Luftwaffe* (Phoenix Mill, U.K.:Sutton Publishing Ltd, 2001); Richard Overy, *The Battle of Britain: The Myth and the Reality* (New York, NY: W. W. Norton, 2000); Stephen Bungay, *The Most Dangerous Enemy: A History of the Battle of Britain* (London: Aurum Press, 2000). The Battle of Britain Historical Society also has a lot of information available at http://battleofbritain1940.net.

[4] Stephen Van Evera observes that a theory must be able to pass a "hoop test" if its predictions are certain; *idem, Guide to Methods for Students of Political Science* (Ithaca, NY: Cornell University Press, 1997), 30-32. These predictions need not be unique (a "smoking gun") if other factors are important for explaining results (*i.e.*, in this case, aircraft or industrial performance in addition to information friction). This case is also "intrinsically important" in the history of World War II and C^2, so it's important to be able to explain it (pp. 86-87).

granular level of detail needed to describe information friction.[5] Detailed process tracing will clarify how the theory's three conditions facilitate C2 performance.[6]

Furthermore, an historical case is valuable because the technological determinist version of RMA doctrine and information friction theory predict opposite outcomes for my two cases. The SOTF in Iraq was a robustly-networked modern RMA organization, and yet IT usage created internal confusion and reinforced patterns of activity there that were, at best, difficult to evaluate, and at worst, counterproductive for the overall U.S. counterinsurgency effort. Fighter Command, by contrast, operated in a pre-digital era with temperamental radar sets, voice radio, and manually-updated maps, yet this network nevertheless produced a then-unprecedented level of shared situational awareness and rapid decision-making which proved critical in defeating the Nazi air offensive. Thus an "information age" organization generated less than stellar results, while an "industrial age" organization achieved RMA-like performance. The difference lies in the relative stability of the problem, agreement about the solution, and capacity to debug operational information systems in wartime. If my theory can provide explanatory value across radically different sociotechnical contexts, then we gain confidence in its generalizability.

Lastly, since data about Fighter Command is part of the historical record, this case provides a crucial validity check for readers concerned about the omissions in my Iraq case due to classification restrictions.[7] There is no need to refrain from discussing specific events and methods. The similarities of information friction across contexts should assuage worries. Frustration with knowledge infrastructures is not just a recent artifact of digital IT usage but part of the intrinsic nature of military C2, whatever the vintage of technology.

---

[5] Air Chief Marshall Sir Michael Knight notes, "Indeed, so much has been researched, written, documented and filmed from all possible standpoints, that there can, in truth, have been only the odd gap, the occasional reminiscence, the last 'recollection in tranquility' to complete the picture," in Henry Probert and Sebastian Cox, *The Battle Re-Thought: A Symposium on the Battle of Britain* (Shrewsbury, U.K.: Airlife Publishing Ltd., 1990), 86.

[6] John Gerring, "Is There a (Viable) Crucial-Case Method?" *Comparative Political Studies* vol. 40, no. 3 (2007): 231-253, argues that while definitive testing with a single Ecksteinian critical case is rarely feasible, "the purpose of an intensive analysis of an individual case is to elucidate causal mechanisms (*i.e.*, to clarify a theory) rather than to confirm or disconfirm a general theory" (233).

[7] I felt it was important to go out and observe contemporary IT usage in combat case because (1) that's where the RMA ought to be most manifest and (2) it isn't well described in public accounts of contemporary operations. Doing so required some compromise in what I could and couldn't describe. By the same argument (about the need to ethnographically document interactions that are invisible or taken for granted among practitioners), there would certainly be a lot of information-processing phenomena that was never documented in 1940. Fortunately, as information theory also expects, some participants in 1940, particularly the operations researchers, were indeed acting as practical ethnographers in their attention to human-IT interaction.

In sum, I selected the Battle of Britain because it's an intrinsically important historical case that the theory *must* be able to explain, and because the wealth of evidence available "under the light" enables me to show information friction in a radically different technological, strategic, and cultural context than in the SOTF case. A success story with rudimentary networks highlights the importance of social context over technical IT capabilities alone.

The first half of this chapter describes how humans and machines shared the widely distributed burden of perceiving, integrating, and articulating air defense information during the battle. The second half explains how the three conditions of information friction theory enabled a strong performance.[8] To sum these up in advance, the British came to understand and stabilize the information problems of air defense during the interwar years, and the Germans inadvertently contributed to the stability of the British system by misunderstanding it (They struggled with considerable information friction of their own!). While there were some challenges in developing political consensus about air defense, especially in Royal Air Force (RAF) ideas about strategic bombing and differences among scientists about the effectiveness of untested technology, these were suitably resolved in time; furthermore, a very centralized Fighter Command provided unity of purpose. Nevertheless, information friction did emerge during the battle as external stability and internal consensus weakened, and yet scientists and military personnel worked closely together to debug the system amidst ongoing operations. The chapter concludes with an assessment of the introduction of new IT in the Battle of Britain and the implications for information friction theory.

8.2 Distributed Cognition in Air Defense

Fighter Command provides an excellent example of distributed cognition, which is where people and machines share the computational burden of constructing representations in order to coordinate action in the world.[9] Much of the computation happened out in the open, rather than hidden deep in software as in modern C2 systems. We can thus trace the ways in which routines

[8] The Iraq case started with the causal conditions and then described distributed cognition (from independent to dependent variables). This case starts with distributed cognition and then causal conditions (from dependent to independent variables). For the Iraq case, I wanted to show how the conditions causally led to information friction, which led to poor performance in a case that is not well understood. For the Battle of Britain case, the effective performance of the information system enjoys broad historical consensus, so I start with that and then test to be sure that the antecedent conditions are what they should be.

[9] Edwin Hutchins, *Cognition in the Wild* (Cambridge, MA: MIT Press, 1995)

and subroutines, standardized formats, aggregative combinations, and error-correcting adjustments enabled people to construct representations that preserved referential integrity through transformation across radio waves, mechanical instruments, map plots, and human minds. The system arranged "cascades of inscriptions" to and from disconnected "centers of calculation" in order to coordinate reliable reconnection with the environment.[10] Fighter Command was successful because it could close its control loop on the Luftwaffe.

8.2.1 The Battle, July-October 1940

After the collapse of France and British retreat from Dunkirk in June 1940, Germany perceived a narrow window of opportunity to invade England. Bad weather precluded invasion in the winter, and a yearlong delay would allow the British time to accelerate rearmament to make the island impregnable. On 7 July Hitler thus directed the Wehrmacht to begin preparations for an invasion codenamed "Sealion." Hitler appears not to have seriously considered this significant and impulsive step prior to the fall of France. While occupation of the French Channel coast would help to counter the Royal Navy's considerable advantages, the RAF remained a prohibitive obstacle to invasion. Sealion was therefore contingent on the Luftwaffe's prior achievement of air superiority, codenamed "Eagle Attack." The Luftwaffe had to defeat the RAF by autumn; the RAF simply had to survive.[11]

Luftwaffe doctrine and capabilities were adapted to support combined-arms blitzkrieg with ground forces, not an independent strategic bombing campaign. Hitler's leading military instrument, like his strategic direction for the invasion, was thus improvised for the task at hand. In summer 1940 the Luftwaffe had three times as many aircraft available for the battle as the RAF, although the more-meaningful balance of combat-ready single-engine fighters was closer to even.[12] The German Me-109 and the British Spitfire were well-matched, although the Me-109 had the advantage at altitude, as well as against the British Hurricane which made up the

---

[10] Bruno Latour, *Science in Action: How to Follow Scientists and Engineers Through Society* (Cambridge, MA: Harvard University Press, 1988)

[11] Overy, *Battle of Britain*, 3-25. A concise summary of the strategic aims and doctrinal posture of the two adversaries is: Barry R. Posen, *Sources of Military Doctrine: France, Britain and Germany between the World Wars* (Ithaca, NY: Cornell University Press, 1984), 94-102.

[12] German bombers and the twin-engine Me-110 were not great threats to Spitfires and Hurricanes in the air (while being quite vulnerable to them), so the Luftwaffe had to destroy the fighters in order to gain air superiority. The balance of serviceable Me-109s to Spitfires and Hurricanes are thus the relevant measure. While estimates of readiness rates vary across sources, it can safely be assessed as no more than 1.5 in favor of Germany.

majority of RAF fighter squadrons. While the British were reasonably concerned about their initial supplies of fighters and pilots, they in fact had greater capacity to produce more of both during the war than the Luftwaffe, which suffered from chronic supply problems; and of course, Luftwaffe pilots who bailed out over England became prisoners of war while British pilots could return to the fight. When we factor in the remarkable British C2 system which enabled Fighter Command to husband its precious fighters, then the net balance tips in favor of the RAF. In the summer and autumn of 1940, the RAF succeeded in the defense for which it had prepared, while the Luftwaffe failed in the offensive for which it had not.[13]

The battle is usually divided into four phases.[14] Attacks on the Channel coast and ports began to intensify in mid-July, although the Germans had staged sporadic raids and patrols to probe defenses in the weeks prior. The second phase began in early August with a concerted Luftwaffe effort to destroy Fighter Command by targeting aerodromes and using bombers as bait for fighters. By the first week of September the Germans believed, wrongly, that the RAF had been defeated, so they launched a coercive bombing campaign against London proper in a third phase known as the Blitz. With the pressure against its infrastructure relieved, the RAF was then able to punish the Luftwaffe, which was operating at the limit of the Me-109's range. The Luftwaffe suffered an unsustainable 25% loss rate during its last major daylight raid on 15 September (commemorated as Battle of Britain Day). Having failed to achieve air superiority, Hitler cancelled Sealion two days later. The fourth phase—the Night Blitz on London—continued into October and then petered out through the winter as Hitler's attention turned toward the Soviet Union. Fighter Command's C2 system put in its most dismal performance during this phase, but luckily the Germans had already given in. Luftwaffe leaders were by then only too happy to get back to their comfort zone, supporting the army in a major ground offensive.[15] The RAF won by not losing.

---

[13] Overy, *Battle*, 29-63; Williamson Murray, "British and German Air Doctrine Between the Wars," *Air University Review* (March-April 1980)

[14] Air Chief Marshall Sir Hugh C. T. Dowding, Despatch submitted to the Secretary of State for Air, 20 August 1941, republished as "The Battle of Britain," *Supplement to the London Gazette* (11 September 1946): 4543-4571, hereafter Dowding, "Despatch"

[15] Horst Boog, "The Luftwaffe and the Battle of Britain," in *The Battle Re-Thought: A Symposium on the Battle of Britain*, ed. Henry Probert and Sebastian Cox (Shrewsbury, U.K.: Airlife Publishing Ltd., 1990), 31

8.2.2 Fighter Command

Britain had the most sophisticated air defense system in the world at the time. It connected multiple types of sensors to detect and track Luftwaffe raids, foremost the "Chain Home" radars, but also visual observers and signals intelligence. Through the centralized accumulation of track data, commanders were able to vector fighters to intercept raids and to alert artillery and civil defense forces on the ground. Tens of thousands of people, military and civilian, worked as functional information-processing components to construct representations of friendly and enemy aircraft and to keep information flowing efficiently throughout the system. Figure 8-1 shows the basic components and hierarchical organization of the C2 system.

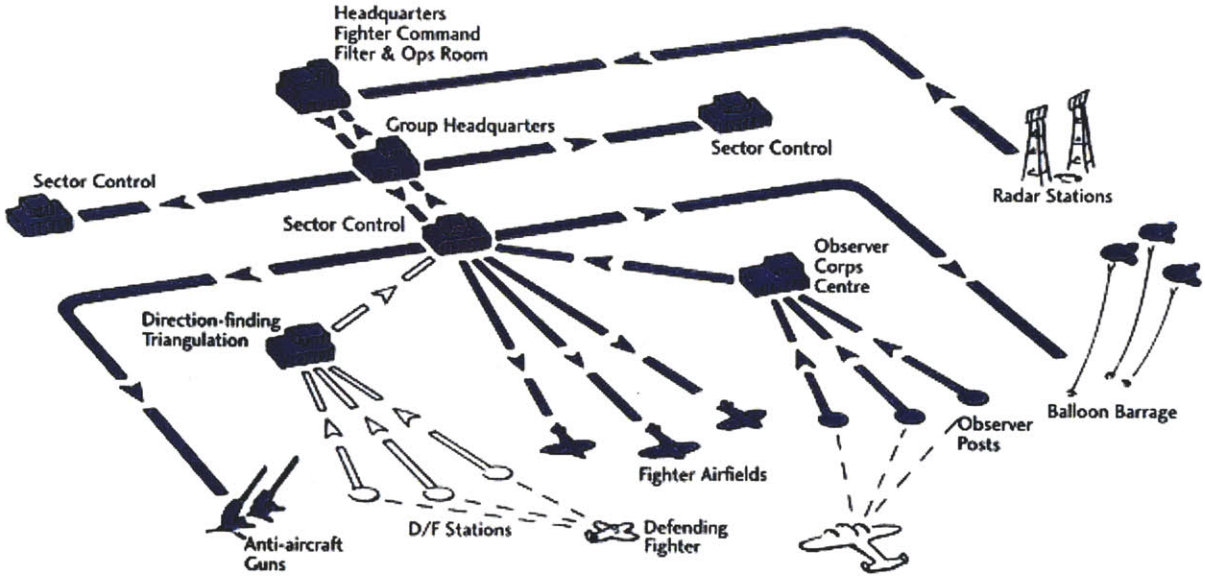


Figure 8-1: Fighter Command's Integrated Air Defense System[16]

Air Chief Marshall Hugh Dowding led Fighter Command since its founding in 1936. Dowding's headquarters was in Stanmore, 10 miles northeast of London, at Bentley Priory. The organization was regionally subdivided into four groups (10/11/12/13), the most important being Keith Park's 11 Group covering London and southeast England, which bore the brunt of German attacks. Groups were divided into sectors, which tactically controlled the fighter squadrons and received reports from the Observer Corps.

[16] Diagram from the RAF's website commemorating the 70th anniversary of the Battle of Britain: http://www.raf.mod.uk/history/fightercontrolsystem.cfm (accessed 5 September 2010).

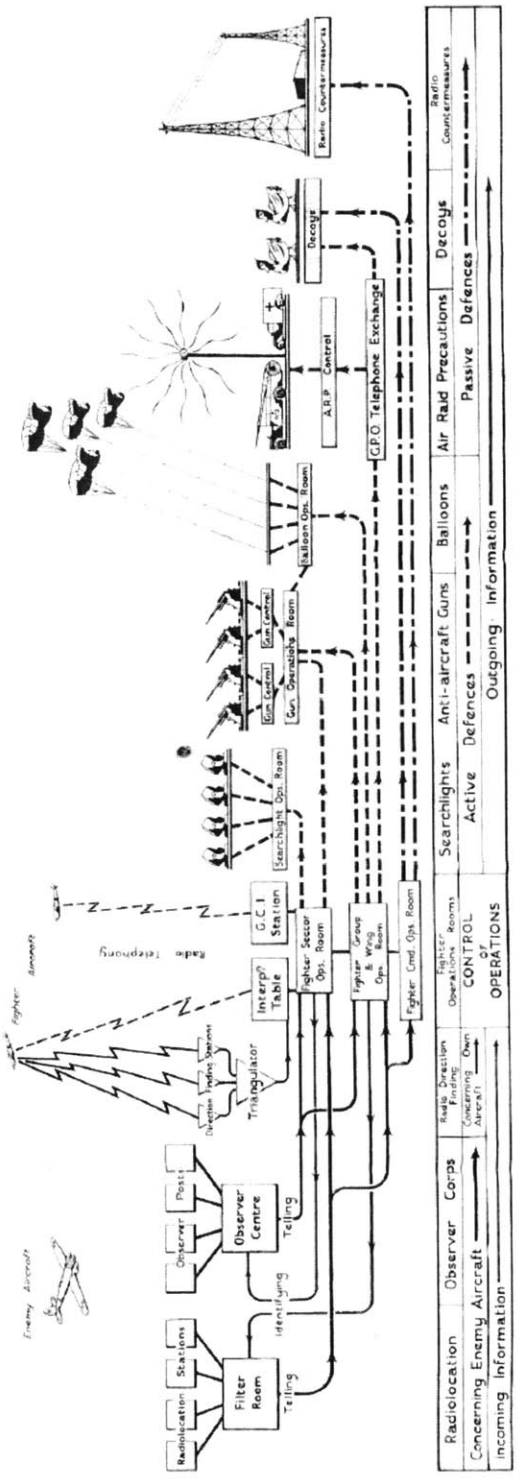


Figure 8-2: "An Outline of Air Defense Organization," Air Defense Pamphlet 1, February 1942[17]

[17] Reprinted in Jon Agar, *The Government Machine: A Revolutionary History of the Computer* (Cambridge, MA: MIT Press, 2003), 211 (PRO AIR 10/3757)

In this hierarchical system, friendly fighter location and observer data flowed up from sectors to group and then to the headquarters Operations Room, where it was combined with radar tracks from the headquarters Filter Room, which received input from all of the Chain Home stations. The Bentley Priory Ops Room compiled an authoritative picture of the friendly and enemy air situation and passed it back down to group and sector Ops Rooms, which controlled fighters, anti-aircraft artillery, barrage balloons, and alerted air raid emergency services. The time between raid detection and the scrambling of interceptors was usually only a couple of minutes.

We can describe the details in terms of the basic phases of control: perception, integration, and articulation. Figure 8-2, from a 1942 RAF pamphlet, illustrates the flow of control through Fighter Command, with perception in solid arrows, integration in boxes, and articulation in dashed arrows. It also highlights how the British relied on a then-emerging discourse of information to conceive of air defense as a rationalized *system* of humans, machines, and organizations.[18] Scientists, RAF officers, and civilians operated and programmed the complex hybrid "information system" which made it possible for Fighter Command to see, think and act. By implementing closed control loops, the entire self-correcting sociotechnical system displayed mind-like qualities above and beyond that of any one member.[19] We will trace the large-scale control problem which Fighter Command as a whole implemented, moving from detection to interception of Luftwaffe aircraft. C2 was successful when the organization could close control loops on the enemy.

8.2.3 Perception

In the perception phase a control system makes physical contact with the environment and creates records of the event. Symbolic records can then be moved to some other place that is not in contact, where records can be manipulated and combined. Fighter Command had to make contact with both enemy and friendly aircraft.

---

[18] *Ibid.*, 209-217

[19] Gregory Bateson, *Mind and Nature* (New York: E. P. Dutton, 1979), 315-319

8.2.3.1 Radar

Radar is an acronym for Radio Direction and Ranging. The British called it RDF (Radio Direction Finding) from 1935 to 1943 to disguise its true function;[20] direction finding was actually a separate technology used to track RAF fighters, to be discussed later. Radar operates on the physical principle that objects reflect electromagnetic radiation and wavelengths longer than visible light, having lower attenuation and absorption rates, can be detected at great distances and through weather. Basic radar concepts were widely understood before the war—Germany had developed individual radar sets with better technical characteristics than British models—but Chain Home was the first to be incorporated into an operational system.[21] Chain Home radars detected the range, bearing, and height of aircraft out to 80 miles, although much greater (or lesser) ranges were possible based on atmospheric conditions, target altitude, and operator skill. They were unable to detect low flying aircraft, so they were supplemented by Chain Home Low stations to detect range and bearing (but not height) of aircraft as low as 50 feet out to 15 miles, and 1,000 feet at 34 miles.[22] At the beginning of the battle there were 21 Chain Home and 30 Chain Home Low stations providing coverage of most of the South and East of Britain, including most of the English Channel out to some Luftwaffe airfields in France.[23] Radar provided Fighter Command with eyes to see aircraft approaching over the ocean.

A Chain Home station transformed physical contact with aircraft (via radio waves) into records of position, altitude, heading, and number of aircraft that could be reported to the Filter Room. The non-trivial process by which radar sets and radar operators mapped real-world physical constraints onto these reportable symbolic quantities involved several intermediary representations. The process is worth tracing in some detail to show how this human-machine hybrid transduced physical contact into symbolic data through a "cascade of inscriptions" that

---

[20] Zimmerman, *Britain's Shield*, 90-91

[21] Alan Beyerchen, "From Radio to Radar: Interwar Military Adaptation to Technological Change in Germany, the United Kingdom, and the United States," in *Military Innovation in the Interwar Period*, ed. Williamson Murray and Allan R. Millett (New York, NY: Cambridge University Press, 1996), 265-299

[22] To detect an aircraft at 80 miles at an altitude of 1,000 ft. using the Chain Home "floodlight" design, the receiving antennas would have to be 1,150 ft. high. Chain Home Low was originally designed as a Coastal Defense radar for ship detection, but it was fortuitously found to be effective against low flying aircraft. Zimmerman, *Britain's Shield*, 171.

[23] Wood and Dempster, *Narrow Margin*, 93

preserved reference to the world through constrained transformations at each step. This is important because when such cascades break then control loops remain open and C2 suffers.[24]

A Chain Home station transmitted a pulsed "floodlight" of horizontally-polarized long-wavelength (12 meter) radiation from wires tensioned between steel towers. Radio echoes from aircraft (which generally flew in the horizontal plane) energized sets of crossed dipole antennas mounted at different heights on a set of wood towers. (Chain Home Low had steerable "searchlight" antennas and a shorter 1.5 meter wavelength.) All of the dipole antennas connected to huts at the base of the receiving towers.

The operators in the huts—many of them members of the Women's Auxiliary Air Force (WAAF)[25]—worked at a console with a cathode ray tube (CRT), a goniometer dial, and buttons that controlled a motorized switchbox, among other things. The x-axis deflection of the CRT beam measured the time elapsed between the transmitted pulse and the receipt of the echo, which was displayed in units of miles (a convenience of the constant speed of light) and thus represented the slant range to the aircraft. The y-axis deflection measured the ratio of the signal strength of two different antennas connected via the switchbox to the stator coils of the goniometer. With the "gonio" switched to connect to the North-South and East-West crossed dipoles, the operator rotated the dial to minimize y-deflection on the CRT, at which point the direction of the dial physically represented the horizontal bearing to the target.[26] This measurement was ambiguous, however, because the crossed dipoles would give the same measurement of an aircraft on a reciprocal bearing; the operator would thus have to toggle reflectors mounted on the tower ¼ wavelength behind the antennas and observe whether the signal increased or decreased to indicate whether the aircraft was in front or behind, respectively.

---

[24] The following account draws mainly on B. T. Neale, "CH: The First Operational Radar," *GEC Journal of Research* vol. 3, no. 2 (1985): 73-83, which provides a thorough technical description of a Chain Home station; Dick Barrett, *The Radar Pages*, http://www.radarpages.co.uk, is also a useful compilation of information about RAF radar equipment and operations; Wood and Dempster, *Narrow Margin*, 88-93.

[25] The RAF considered women to have "higher power of sustained concentration on a limited field of observation devoid of 'entertainment value'...finesse in relatively delicate setting of light moving parts...general conscientiousness...lower average tendency to magnify individual importance by partial disclosure of secrets" and could thus "release men for other duties," Zimmerman, *Britain's Shield*, 167. Direct combat work was for men while indirect information work became "women's work" and thus somewhat invisible next to the more harrowing tales from the cockpit. On the gendered origins of computation, see Jennifer S. Light, "When Computers Were Women," *Technology and Culture* vol. 40, no. 3 (1999): 455-83

[26] Minimization provided the cleanest CRT display. For weak signals the operator could maximize deflection, which required an additional 90° correction for the horizontal measurement.

(Clearly this system required much more manual intervention than with the more familiar Plan Position Indicator—PPI—display, which represents range and bearing on a polar plot with signal strength represented by intensity as the beam sweeps around; PPI only became available towards the end of the battle.) When the "gonio" was switched to connect to dipoles mounted at 215 feet on the tower and another set at 95 feet, the operator could measure the vertical azimuth to the target by a similar process. The "long afterglow" display of the CRT enabled the operator to distinguish the reflection signal from background noise and jamming because unsynchronized transient noise didn't build up a signal. Experienced operators could count aircraft in formation by observing the beat rate of the echoes on the display; a button on the console could momentarily shorten the transmitted pulse from 20 to 6 microseconds, which improved range resolution. The operator also attempted to classify the contact as friendly or not based on a distinctive return pattern generated by a transmitter that most RAF airplanes carried, called Identify-Friend-or-Foe (IFF). Furthermore, the operator had to continually tune the apparatus as conditions changed; for example, she had to switch between measuring echoes from the main transmitter (centered at 5.2°) and a gap-filler transmitter (centered at 5.9°) if the aircraft climbed out of the main lobe of former. Mindful attention and active intervention was needed to get the instruments to represent features of the world on their displays.[27]

As the operator read off these various representations, other personnel logged the measurements. When they had a complete set, they then performed some difficult trigonometric calculations using several site-specific correction parameters (extensive calibration effectively pre-computed part of the problem prior to runtime) in order to convert the ranges and angles into grid coordinates and altitude. At first these were performed manually on paper and a plotting board, but this tedium was soon replaced with a purpose-built mechanical tabulating device called "the fruit machine," much to the relief of station personnel.[28] The computed coordinates and altitude thus obtained, along with the IFF reading, heading and number estimate, was "told on" via landline voice telephone to the Filter Room. Later in the war, some of this

[27] Neale, "CH," 76, describes the intuitive skill required: "Signals at extreme ranges, well below 'noise' level, were detected and tracked. The mechanism by which this was achieved is still not fully understood but believed to be due to an unconscious form of pattern recognition within the noise structure, somewhat analogous to the 'cocktail party' effect. "

[28] Zimmerman, *Britain's Shield*, 185; Wood and Dempster, *Narrow Margin*, 90. Hopefully the "fruit machine" results were less random than a slot machine, although it's a fitting metaphor for the noise inevitably introduced in the Chain Home implementation.

communication would be further automated by connecting some of the radar console and "fruit machine" outputs directly to teletype printers in the Filter Room. In such instances the humans could offload some information-processing tasks onto the machines once the tasks became well and discretely defined formal operations (but of course human labor then shifted over to programming and maintaining devices like the "fruit machine"). Many of the operators' situated, intuitive, interpretive performances were not so well defined, however, and thus the radar stations relied on considerable human connective tissue amongst the machines in order to propagate state.

To summarize the transduction of the world's state to the station's symbolic output: the airplane's movement was constrained by the relations between rate, time and distance and its physical construction and movement through the sky; the radio-illuminated aspect of this situation then propagated to the antenna, where it was represented in the switchboard-configured electrical activation of the antenna; the analog deflection of the CRT and angular setting of the goniometer amplified and thus parsed out more specific features of this energy; the operator read and logged these as symbolic values, then transferred them to the mechanical state of the pre-programmed "fruit machine," and then read the newly computed values back out to the log and plot; finally the symbolic data resonated in the voice of the "teller" through the telephone to the Filter Room. At each step the representations became more discrete and less attached to a particular locality, and at each step humans bodily facilitated the movement of information across media as they mindful worked to faithfully re-represent real-world constraints across each transformation.

The radar station was a black box providing data for the Filter Room. Any control loop in an organization involves nested control (loops within loops). For example, a radar operator perceived the instrument readings, integrated them in her mind, and manually articulated adjustments to the apparatus in order to obtain the range and bearing to a contact, yet this was all part of the perception phase of the larger-scale loop which connected the radar to the filter room. The hybrid human-machine implementation occasionally broke through the simple abstraction of radar-as-symbolic-location-provider, as will be discussed below. The complexity of implementation at even this primary stage of perception suggests that the commonly used data-

information-knowledge distinction is misleading: complex knowledge work is involved even in producing basic data. One person's data is another's knowledge.

8.2.3.2 Observer Corps

Radar tracked aircraft over the ocean. Once they crossed the coastline they were tracked visually by a network of 30,000 observers at 1,000 observation posts. The Observer Corps ("Royal" was prefixed in 1941) was a civilian volunteer organization whose enthusiastic members endured countless hours of boredom and exposure to the weather on hilltops around England. Churchill denigrated the system as "Early Stone Age," but it was a much better-organized version of the system employed in the First World War. Over a million observation reports per day (an average of a thousand per post) flowed up to Fighter Command headquarters, with transmission times via the intermediate observer centers as fast as 40 seconds.[29]

As with radar, observers relied on mechanical devices to transduce visual connections into reportable symbolic data. Each post had a sextant-like instrument mounted at the center of a ten-mile radius map, which displayed a coordinate grid and the five-mile circles of any other nearby posts. On sighting an aircraft—binoculars and ear horns amplified its signature somewhat—the observer had to estimate the altitude, which depended greatly on skill and experience. If the sighting had been cued by an observer center following a radar track approaching the coast, then the center might be able to provide an altitude to assist the observer in the initial detection and height estimation. If a neighboring post could also see the aircraft, then they could, together via telephone, use a device on the instrument to obtain the height by comparing their respective azimuths to the contact. The observer would then set a bar representing the height and rotate the instrument and adjust the sight angle to point at the aircraft, which drew a pointer to a 2-kilometer grid square on the map. The post then logged and called in to their center via telephone the formation's count, direction of flight, height, and map grid square read off the instrument. Many also attempted to identify the aircraft, tending to err on the side of designating them hostile. For sound-only contacts they passed the bearing and apparent direction.

The observer post was distributed cognition at its simplest. The sextant transformed a hard cognitive trigonometric task into simpler perceptual one. The processing load was

[29] Wood and Dempster, *Narrow Margin*, 96-98

distributed across people—neighboring sites, observer centers, instrument manufacturers and cartographers—and across time, in the pre-computing of map data and the sequential setting of the height bar in order to plot the location. The precision of the instrument and its structural correspondence to a larger scale physical relationship in the world allowed the post to manage more relationships more quickly than they could do with their minds alone. Here and throughout Fighter Command, people offloaded mental processing onto their tools and together computed solutions to representational problems. As with radar, the stereotyped and repetitive nature of these tasks made them ideally suited to mechanical assistance, yet still required active mindful intervention from the operator in order to perform in such a way that the entire post could act as a black-box sensor for upstream C2 nodes.

8.2.3.3 Signals Intelligence

Britain operated several stations to intercept German radio transmissions; they could not connect with Luftwaffe landline communications. Bletchley Park or "station X" broke high-grade encryption by the German Enigma machine, which became "Ultra" intelligence. Ultra was sanitized before being sent to Fighter Command in order to disguise its origin and thereby protect the Allies' most valuable and secret source of intelligence.[30] While it provided some information on Luftwaffe order of battle and readiness, Ultra was of little tactical use because it took too much time to decrypt and figure out who needed to know.[31] Low grade ciphers and clear-voice transmissions processed by the RAF's "Y" service were far more useful. Luftwaffe security discipline was lax; for example, before the war they actually painted their unit name and radio codes on their aircraft, so when they finally repainted and changed codes at the start of the war, British Air Intelligence was easily able to recover the organization. Y intelligence, reported from Cheadle station to Fighter Command HQ, provided operational warning that a raid was

---

[30] Bletchley Park "was a factory that worked on symbols and paper. And the direction symbols traveled was from uncertainty to certainty, culminating in the 'unambiguous language of complete objectivity,' as a Hut 3 officer described the end products," Agar, *Government Machine*, 209. For a good account of the workings of the station, see Christopher Grey and Andrew Sturdy, "A Chaos That Worked: Organizing Bletchley Park," *Public Policy and Administration* vol. 25, no. 1 (2010): 47-66.

[31] The official British history of intelligence in the war states that, "for all his major decisions C-in-C Fighter Command accordingly depended on his own strategic judgment, with no direct assistance from the Enigma," cited by Wood and Dempster, *Narrow Margin*, 77. F. W. Winterbotham, *The Ultra Secret* (New York, NY: Harper & Row, 1974), claims that Ultra was critical in the battle, but this claim is generally disputed; see Edward Thomas, "The Intelligence Aspect," in Henry Probert and Sebastian Cox, *The Battle Re-Thought: A Symposium on the Battle of Britain* (Shrewsbury, U.K.: Airlife Publishing Ltd., 1990), 42-46.

being launched and sometimes tactical information to assist in vectoring fighters.[32] The British also exploited a German navigational beacon called Knickebein ("bent leg") which guided Luftwaffe bombers to within 500 feet of their target. Its existence was discovered on 17 June 1940 through interrogation of a downed Luftwaffe pilot. The British figured out how to detect its direction for early warning against specific targets and, in August, how to spoof and jam it, after which German pilots lost confidence in it.[33]

Like radar and the observers, intelligence collection exploited physical constraints to transduce radio contact into detachable symbolic records. However, the environmental stabilities that made its representation possible included not just physical phenomena but also the organizational routines of the Luftwaffe. This was of course true to a lesser degree for radar and observers—insofar as low altitude raids, weather and night flying, and diversionary feints could confuse perception—yet these sensors should be considered more primary sources of representational cascades because they made contact with some fairly substantial and hard-to-change objects and phenomena. Intelligence, by contrast, was parasitic on existing cascades of inscription: it made copies of the representations generated by the enemy's perception-integration-articulation loops. To the degree such loops were stable (and thus meaningful) for the Germans, then the British could use them in their own stabilized control loops. Yet because the ultimate end of the latter was to destabilize the former, action on intelligence could be self-negating. Worries about this fundamental action-security dilemma at the heart of the intelligence problem resulted in additional counterintelligence complexity piled onto this particular perceptual stream—such as sanitization and "need to know" certification—that limited its usefulness. The reason to make representational cascades in the first place is because symbolic records are easier to move around and manipulate than the more substantive things the organization needs to coordinate. This makes the stability of those records-in-context more flimsy than durable objects and physical phenomena; therefore, perception channels that depend

---

[32] Aileen Clayton, *The Enemy is Listening* (New York, NY: Ballentine Books, 1982) provides a first-person account of the RAF Y service.

[33] Sebastian Cox, "A Comparative Analysis of RAF and Luftwaffe Intelligence in the Battle of Britain, 1940," *Intelligence and National Security* vol. 5, no. 2 (1990): 425-42; Wood and Dempster, *Narrow Margin*, 73-77

more upon connection with the former (like signals intelligence) will be inherently less stable than that which depends more upon connection with the latter (like radar).[34]

8.2.3.4 Radio Direction Finding

If intelligence is unstable because the enemy can readily change the very information-processing routines it targets, then the same sources and methods will be considerably more stable if the target routines are under friendly control. Fighter Command needed to detect and track not only enemy raids but also its own fighters (today known as "blue force tracking"). This was accomplished with high frequency (HF) radio sets in the aircraft which would automatically transmit a 1,000 Hz note every minute (earning it the name "pip-squeak"). This signal was detected by three antenna towers at a direction finding (DF) station located in each sector. In the station there was a plotting table with a map and three weighted or elastic strings, each connected to the location of a tower. There was an operator for each antenna who measured the bearing to the aircraft by tuning a goniometer to the strongest signal. Each then pulled his string along the map using protractor marks along the edge of the table. A fourth operator plotted the intersection of the three strings (which formed a "cocked hat") and "told on" the triangulated position of the fighter to the DF plotter in the Sector Ops Room. The process took 14 seconds, and so the aircraft "pip-squeak" was designed to transmit for 14 seconds every minute. By synchronizing the transmitter via the Sector controller with a stopwatch, it was thus possible for one DF station to track four aircraft at once. Generally this meant that they tracked four squadrons at once, assuming that a squadron flew in formation.[35]

The DF station acted as a black box for sensing aircraft coordinates, much like the other sources of perception examined above. Yet this further highlights the way in which there were control loops within loops. The four airmen were clearly in the integration phase of a control cycle which began with the perception of three radio signals and completed with the articulation of the fix. While in some sense the three signal bearings contained all the information necessary to fix the position of the aircraft, that solution was not really available until each airman bodily moved them onto the map and satisfied some specific constraints: one constraint was met by

---

[34] The growth of more sophisticated radar and electronic countermeasures turns even radar more into a problem like intelligence, where both sides struggle to protect their own and exploit the information processing of the other. Yet the durable "thing-like" aspect of an aircraft target compared to the more changeable "idea-like" aspect of a record target is still a significant difference.

[35] Zimmerman, *Britain's Shield*, 158; Wood and Dempster, *Narrow Margin*, 108-113

literally attaching the string to the map and another by drawing the string taught to meet the number on the protractor that matched the bearing reading. The constrained propagation of multiple representations onto the structured space of the map constructed a new multi-source "fused" representation in the form of plotted coordinates, thus guaranteeing that this new aggregate representation stood in a particular relationship to the state of the world (at the time the bearings were read).[36] Unconstrained degrees of freedom in the transformations and combinations—distortion in the signal, fidelity of the goniometer, operator competence, the area of the "cocked hat," *etc.*—undermined that guarantee. All of the processes of perception reviewed here involved many control subcycles along the way, some like the Bletchley Park "module" involving far more complexity than others.

8.2.4 Integration

Integration is the knowledge management phase of the control cycle. It "performs a kind of translation, from perception to articulation,"[37] by comparing and combining multiple information streams with one another and with information in memory to produce new refined information to exert downstream control. A military command center performs integration in a "center of calculation" which usually features an authoritative and panoptic representation like a map or database. This site facilitates combinations of inputs, provides state-based memory by virtue of its path-dependent construction, and provides a miniature model of the outside world that personnel can gather around to observe all at once.[38] Commanders use the state of the map to make sense of the state of the world and to figure out how they would like to intervene in it in order to change it and to bring it closer into alignment with their mission objectives.

8.2.4.1 Communications

Centers of calculation work because they have the freedom to rearrange symbolic representations in a disconnected state in order to arrange some later reconnection. Fighter Command had a reliable and redundant communication system to facilitate the frequent reconnections between all of its partially-disconnected information-processing nodes. The

---

[36] Hutchins, *Cognition in the Wild*, 125-127, describes a similar constrained transformation of representation in a ship plotting its own location (rather than DFing a target).

[37] Mindell, *Between Human and Machine*, 23

[38] Paul N. Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America* (Cambridge, MA: MIT Press, 1996), uses the "closed world" metaphor to describe military centers of calculation in order to emphasize their insulation from reality; the phrase understates the interest personnel often take in the pragmatic alignment of representation and world.

General Post Office created Defense Telecommunications Control to keep up a variety of communications pathways: dedicated landline telephones, switches to the civilian network, emergency radios, *etc.* A teleprinter network was also installed to automatically transmit intelligence reports, combat reports, pilot and equipment replacement requests, damage assessments, and increasingly, information directly from its far-flung sensors. Human "tellers" at every C2 node functioned roughly like modern-day routers to transfer information to the appropriate addresses.[39]

8.2.4.2 Filter Room

Chain Home radar stations connected to a central Filter Room in Bentley Priory. Reports from individual radar stations were unreliable due to the vagaries of site-specific calibration, variable operator skill, atmospheric conditions, and genuine ambiguity about raid composition and identity. The "searchlight" design of Chain Home guaranteed a lot of overlap among the stations (which were sited about 20 miles apart), and different stations varied in what they reported for the "same" contact. A "filterer" linked by telephone set to a station plotted every report. A messy spider web of plots usually emerged, many of them tracing a zigzag path when a station measured successive target positions and headings erratically. Chain Home height measurements were especially unreliable. The filterers assessed the probable qualities of the plots, threw out those that appeared to be erroneous, and joined and straightened those they believed were legitimate. To perceive patterns out of the mess of plots required considerable technical knowledge of radar, experience filtering, and acquaintance with the idiosyncrasies of individual radar stations. In short, the radar station interface abstraction was "leaky," and the filterer had to compensate for its particular implementation. The filterer's intuitive judgment was christened an official track, marked by a token placed on the map. It was given a number and assigned an "X" if unidentified, "H" for hostile and "F" for friendly, another intuitive judgment that depended on fickle IFF reports, the origin and course of the track, and information from the Ops Room on friendly fighter locations. The official track and all updates to it as they

[39] Wood and Dempster, *Narrow Margin*, 117

were received (and fused with the same intuitive pattern-matching) were passed to the Ops Room right next door and "told on" to the group Ops Rooms by phone.[40]

The Filter Room was an integrative center that sorted, compared, and combined incoming data from the stations with information held in the "memory" of the state of the plotting board and the minds of the filterers, translating this all into a validated track. Messy records became cleaner records, and an "objective" picture of the airspace started to emerge for the first time. From the Ops Room's perspective, of course, the integrative work of the Filter Room was bundled up into a black box for perceiving actual tracks. The Filter Room was a critical buffer between the messy particularity of radar stations and the cleaner abstraction of "the track" in the Ops Room. In fact, the filterers were working through information friction generated by the uncoordinated and non-standardized idiosyncrasies of stations. Their job was to protect the Ops Room from information friction and instead present a clean symbolic track free of equivocation. An inevitable problem with such cleaning was that provenance linking the symbol to its messy origin was also discarded, and the resultant track might thus appear far more clean and reliable in the Ops Room than it should have; later we'll discuss some fratricidal tragedies that resulted.

8.2.4.3 Observer Centers

Each sector had observer centers which were essentially like filter rooms for a few dozen observer posts. The "Sea Plotter" accepted radar tracks (via the Ops Room) that were approaching the coast, since these would have to be tracked over land by the Observer Corps.[41] Twelve plotters sat around a map table, each connected via a head and breast telephone set to a couple of posts. They alerted posts of impending flights. For each report they received, they placed markers on the map which pointed in the direction of flight and displayed the number of aircraft in red, the track number assigned by the Filter Room (and passed via the Ops Room) in white, and the altitude in 1,000s of feet ("angels") in blue. They marked flights missed by radar with a special code for their territory. When new reports came in they moved the markers in five-minute intervals, placing an arrow marker at the previous location to "remember" its path. A floor supervisor checked the plots, and tellers on a raised platform phoned information to

[40] Neale, "CH," 81; Derek Wood, "The Dowding System," in Henry Probert and Sebastian Cox, *The Battle Re-Thought: A Symposium on the Battle of Britain* (Shrewsbury, U.K.: Airlife Publishing Ltd., 1990), 5; Wood and Dempster, *Narrow Margin*, 89, 118.

[41] Wood, "Dowding System," 5, notes that they weren't supposed to know about radar but it was obvious they did from the rude remarks in their logbooks.

group and sector Ops Rooms, while a recorder traced out more permanent records. The "centre staffs *worked like machines* to convert [observer reports] into plaques and arrows and pass the information to the Fighter Group headquarters."[42]

8.2.4.4 Operations Room

The Fighter Command Ops Room was perched at the apex of cascades of inscription flowing up and down the organization. It consolidated the single authoritative air picture from all sources of information. WAAFs wearing telephone headsets moved tokens representing the radar and observer tracks of both raids and friendly airplanes around the map with "croupier rakes." A slotted blackboard (the "totalisator") displayed squadron availability and assignments against particular raids, which kept the plotting table clear except for the numbered raids and interceptor tracks. Officers on a raised balcony had a panoptic view of the island's airspace and telephone links to Group and Sector Ops Rooms.[43] The Fighter Command Ops Center was one of the first true "all source fusion" centers, predating a similar achievement at the Admiralty for tracking submarines.[44] The abstract analog of Britain's airspace housed in the Ops Room table was the critical linkage between Fighter Command's ability to detect and to intersect the Luftwaffe.

Standardized formatting was essential for passing information between the Filter Room, Observer Centers, and HQ, Group, and Sector Ops Rooms in order to maintain actionable plots. Indeed, the bureaucratic standardization of information is *the* key move that enables any sort of "seeing like a state."[45] All stations used the same gridded map scheme so they only had to pass the code for a given 2-km square. They all had clocks on the wall with each five-minute segment color-coded. When plotters updated a track, they looked to the clock and chose a token that matched the current color. Only three colors were allowed on the air picture at any one time to ensure that information displayed was never older than 15 minutes. Track markers were

---

[42] Wood and Dempster, *Narrow Margin*, 105 (emphasis added), 89, 98
[43] *Ibid*, 110, 116
[44] Patrick Beesley, *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Center 1939-1945* (London: Greenhill Books, 2000)
[45] James C. Scott, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed* (New Have, CT: Yale University Press, 1998)

standardized, with different shaped tokens for different types of aircraft. Telling procedures were strictly specified with a standard reporting order and pace of speech.[46]

This standardization was an agreement in advance about what categories and properties of things would matter at runtime. The resulting representations picked out very particular aspects of the world (raids and interceptor squadrons composed of multiple aircraft moving along a given vector and altitude, *etc.*), and intentionally kept anything else off the board. Standardization was also an advance agreement on how exactly each transformation of one type of representation into another would be constrained so as to preserve referential integrity to the aspects that mattered. Standardization enabled a great deal of speed and flexibility in passing details on changing tracks across all the different C2 nodes, with some confidence that plots were actually coordinated with what was happening in the sky. Flexibility and confidence, that is, as long as tracks and interceptions were the only things people wanted to discuss.

This brings up the critical matter of the organization's goal. A cybernetic circuit is usually described in terms of sensing the state of the world (perception), comparing it with a goal state (integration), effecting action to reduce the difference between the two (articulation), and measuring the new state of the world to begin the cycle again (feedback). Dowding and Park understood Fighter Command's primary mission to be its own preservation, rather than the immediate protection of London, because failure to survive would just open London to invasion and far worse destruction. Survival implied two tasks: to avoid getting sucked into costly fighter duels with predatory Me-109s, but also to impose enough loses on the Luftwaffe to convince Germany to abandon the attack. Fighter Command was in a battle of attrition, so it had to be able to both endure attacks indefinitely and also to cause attrition for the enemy. These goals were operationalized by pairing raids with interceptors for the most favorable tactical engagements. Ops Rooms measured the gaps between hostile and friendly aircraft tracks as well as the gaps between their actual and tolerable wastage rates. The panoptic layout of the Ops Room—the air situation and the "tote" board—was designed for commanders to be able to visually make these measurements from the gallery and to make decisions about which gaps to close by articulating orders. It was not designed for them to pick targets for Bomber Command, assess the damage in London, or track civilian passenger flights to their destinations. The

[46] *Ibid*, 118; Dowding, "Despatch," 4547; Agar, *Government Machine*, 214

standardized categories and processes of representation supported the particular types of measurements, comparisons, and articulations Fighter Command needed to perform in order to register and reduce interception and wastage gaps in support of its defensive strategy.

The shadow of the world cast on the wall of the Ops Room cave (literally in a bunker) was the filtered world of things that Fighter Command could actually act on. Its potentials for action structured its processes for perception. Insofar as Fighter Command's strategy was well suited to counter the Luftwaffe, this sort of structured and constrained seeing enabled it to effectively implement its operations. It is critical to appreciate that the Ops Room's single air picture was not just a value-free analog of the world, but rather a literal integration of its purpose-built channels for perception and action.

8.2.5 Articulation

Articulation is like perception in reverse. Perception transforms the state of the world into symbolic records though constrained mappings from one media to another, across machine, human, and paper boundaries. Articulation—the word evokes a jointed apparatus and precision of speech—progressively transforms disembodied symbols into increasingly particular local situations. It facilitates reconnection with the world in order to change it and to improve control.

8.2.5.1 Sector Ops Rooms

The HQ Ops Room "told on" its air picture to the groups, and the groups told the sectors. Groups and sectors had Ops Rooms which were organized similarly with a plot, "tote" and radios, but on a smaller-scale to represent only the areas and squadrons they managed. Just as the perceptual circuit moving up to HQ involved loops within loops and intermediate integration centers, so too did the articulation circuit moving down. The group and sector Ops Rooms were, in fact, also integrative nodes on the perceptual circuit insofar as they aggregated and reported observer data and squadron locations from the DF stations; here, however, we'll just consider a sector Ops Room's role in transforming symbols into substantial action.

While a sector Ops Room indeed had a small-scale resemblance to the HQ Ops Room, it actually displayed more fine-grained information. For example, in addition to the "tote" board, the sector also had electrical "state panels" with four-foot high boxes for each squadron displaying six colored lights representing different states of readiness. In the movement down

the articulation circuit, HQ's abstractions had to be materially implemented. Representations became more tied to a particular situation and locale.[47]

The sectors also had to deal explicitly with the problem of time. As with any articulation, their job was to arrange a *future* reconnection with the world. They had to compensate for the fact that their plot had been constructed in a relation to a past state of the world, or at best an estimate of its current state. The last radar or observer fix might be a minute old, and it might be minutes hence before a squadron could intercept a raid. Dead reckoning was the only solution to this problem. The plot of past activity was extended out in a constrained manner to estimate the future position of the same activity, based on a model of how it should evolve in the mean time. The trigonometric problem of calculating an intercept path for two non-maneuvering aircraft is a two vector problem that can be quite complicated. Sector Ops Room personnel used a neat heuristic to simplify the problem. By the "Principle of Equal Angles," affectionately known as the "Tizzy Angle" after Henry Tizard who worked it out, the controller plotted—or simply visualized if experienced enough—an isosceles triangle with the baseline linking the interceptor (DF plot) and the raid (hostile track) and the raid's track as one of the edges. By extending the interception course out at the same angle to the baseline, the controller could provide a heading to the apex of the triangle where the interception should occur. Since fighters were at least as fast as the bombers, they could get there first and take a favorable attack position above. If another fix came in the mean time that indicated that the raid had changed course, the controller simply visualized a new triangle and revectored the interceptors. The Tizzy Angle is another example of turning a hard cognitive problem into a simpler visual problem, although interestingly part of the representation was in the controllers' minds once they dispensed with actually plotting triangles. It worked because the constrained transformation of one type of representation (the current track plot) into another (the new heading) recapitulated the real structural constraints on the trajectory of aircraft. The mapping failed, of course, if the target maneuvered; the structured feedback loop (through radar and the Filter Room) enabled the controllers to correct their mapping.[48]

---

[47] Wood and Dempster, *Narrow Margin*, 119

[48] *Ibid*, 112; Zimmerman, *Britain's Shield*, 116

Later in the war the British adopted ground control intercept (GCI) techniques that used PPI radar displays that could display both the target and the interceptor on a two-dimensional display with a sweep and afterglow. When plotting the two tracks independently in the method described above, any accumulated errors in position or heading of either contact could botch an interception. When they were displayed in relation to one another on the same radar image, however, then the errors in the representation would be the same for both contacts, thus preserving the meaningful relative relation between them. This is yet another of many instances of IT automation of cognitive work and of the transformation of cognitive into visual problems. Height remained a difficult problem even with PPI.[49]

The controller maintained authority over the squadron, vectoring their bearing and altitude, until the flight leader gained visual contact with the raid. Prior to visual contact, the sector HQ actually had a better idea of exactly where the fighters were because of the DF plot (unless the sector had to control more than four squadrons, which was a stress case demanding careful dead reckoning and concentration to keep track of them all). Years before the war pilots used to have to navigate and report their positions regularly, so DF tracking essentially offloaded the cognitive load of pilot navigation onto an entire external organization to allow the pilot to focus on other things like impending combat. Controllers, furthermore, were former pilots themselves, which helped them to create trust over the radio, detect nuances of jargon and tone of voice, and to enable the controller to better simulate in his mind what the fighters were experiencing. The common experience between the pilot and the controller was a form of standardization which stabilized this critical information channel.[50] Once the interceptors had visual contact, the controller generally transitioned to a monitoring role.[51]

8.2.5.2 Fighter squadrons

The C2 system could place fighters in a position to intercept a raid, but it was up to the squadrons to finally close the loop. The dramatic aerial maneuvers and tight control loops of the close-in tactical fight were only faintly legible to radio controllers and DF plotters miles away in their closed worlds. It was nonetheless still a matter of distributed cognition for pilots scanning

---

[49] Dowding, "Despatch", 4560

[50] The U.S. Air Force requires operators of remotely piloted aircraft like the Predator drone to actually be certified pilots, on a similar line of argument.

[51] Wood and Dempster, *Narrow Margin*, 113, 121

the sky ("head on a swivel") and their instruments while communicating with one another over tactical radio, but it was a tighter and quite particular problem. The large-scale uncertainty over the interception was reduced as the airmen pushed forward to a position where tactical control loops could gain traction on the very dynamic structure of the situation. When a problem is uncertain, pushing people closer into it creates smaller-scale problems for them in which they might recover certainty. The process of articulation ultimately culminated in the world of aerial combat becoming its own representation, with pilots desperately managing their relative positions within it.

As in the Ops Rooms, prior design-time standardization enabled speed, flexibility, and accurate communication at runtime. Pilots used radio brevity codes to refer to "bandits" at so many "angels" (thousands of feet), "tallyho" at the merge, "pancake" to return to base, *etc.* Such phrases, keyed to standardized tactical routines linked to recurrent patterns of air combat, enabled the squadrons to combine tactics in novel ways as the fight developed. Prior coordination could also standardize new interpretations intended to deceive German intelligence; for example, "Angels 18" might actually mean "go to 21,000 feet," to lure a listening enemy to a disadvantageous lower relative altitude.[52] Standardized procedures relied on prior coordination in time to structure and simplify activity in space. A prior and substantial logistics effort—not strictly pre-computational but critical for the machinery of articulation—furthermore enabled this performance: "refueling, rearming, engine checking, including oil and glycol coolant, replacing oxygen cylinders, and testing the R/T set would all go on simultaneously" with an 8-10 minute turnaround day and night, out in the open to avoid Luftwaffe attacks on hangars, dispersed, in a blackout.[53] Prior effort in time structured highly dynamic interactions in space.

The perception/feedback phase of Fighter Command's control loop was already active during the culmination of articulation. Controllers monitored the radio in case it became necessary to order an end to the attack, send in reinforcements, or prepare for raids that leaked or punched through the screen of interceptors. When the pilots returned to base they filled out combat reports describing friendly and enemy losses (usually exaggerated), the effectiveness of

[52] Dowding, "Despatch," 4548
[53] Wood and Depster, *Narrow Margin*, 226

searchlights and artillery in illuminating or breaking up a raid, and so forth.[54] Fighter-mounted television cameras provided a gun's eye view of the interception, which was invaluable for debriefing and training aircrew.[55] Every contact with the enemy was an opportunity for further perception and further tweaking of the architecture of control, all with a view towards the reliable and repeated closing of the loop on the enemy. The C2 system measured and closed gaps between the state of representations and the state of the world.

8.2.5.3 Ground Defenses

Fighters were Britain's primary means of defense, but the sectors also activated supporting defenses. Searchlights lit the night sky for fighters and artillery. Artillery barrages placed flak in the path of raids prior to the arrival of interceptors (thus the need for careful DF plotting and synchronization by the sector controller to avoid fratricide). Listening stations helped to aim searchlights and artillery. Balloon barrages lifted to force bombers up to higher altitudes in order to interfere with their targeting accuracy (Dowding thought that balloons were of limited tactical utility, but "they exercise a very salutary moral effect upon the Germans"[56]). Decoy airplanes, hangars, and factories further confused German targeting. Lastly, sectors alerted civilian emergency services to prepare to deal with the consequences of bombing: a "yellow" alert twenty minutes out gave first responders time to prepare; a "red" alert triggered air raid sirens to warn the general populace of an impending raid; "green" signaled all clear.[57] All of these tactical functions had their own miniature Ops Rooms to manage their specific translation of symbols into effects.

8.2.6 Results

Historians largely agree that Fighter Command's C2 system was a remarkably important factor in the British victory. Because Dowding and Park could judiciously place their fighters in the path of the raids which they judged most threatening, they were able to use their precious supplies of pilots and machines to maximal effect. Because they could thus husband their fighters and still damage the Luftwaffe, the Germans failed to achieve air superiority. This failure meant that Hitler had to cancel the invasion, even though Germany was probably never really capable of it anyway, given the great difficulties of and German lack of preparation for

---

[54] *Ibid*, 206
[55] Dowding, "Despatch," 4558
[56] *Ibid*, 4546.
[57] *Ibid*, 4547

amphibious assault of the island. Proving that, however, would have been far more costly than the battle actually was. Certainly the battle was good for British morale.

The system was obviously not perfect, for the battle was still "a close run thing." Over 40,000 Britons were killed in the battle and the Blitz. The RAF lost 1,032 fighters to the Luftwaffe's 1,011. Nonetheless, the defensive shield bought time for British industry to make good those losses, maintaining steady fighter availability throughout the battle, while the Luftwaffe was whittled down to 533 serviceable fighters by early September.[58] In the respite thus won, the RAF started to plan its own strategic bombing campaign against Germany, something for which it would prove far less prepared than it had been for the defense of Britain.

We now turn to the various challenges involved in preparing and operating this successful defensive system. Accepting that it was successful, we need to test whether it meets the three conditions that information friction theory says are necessary for effective C2.

8.3 External Stability of Air Defense

Successful C2 depends on stable control cycles that reliably and repeatedly close on the enemy. There are two aspects of stability: at the "objective" pole are the battlefield and the ability to connect with it in principle; at the "subjective" pole are the organizational and representational resources which make integrated control possible. There is something to know and there is a process for knowing. The first two of the three conditions for successful C2 in information friction theory take these two aspects in turn, even though we should recognize their mutual influence. British understanding of air defense as stable and solvable emerged historically right along with struggles to establish consensus about the solution: the problem was not just inherently stable, but was actively stabil*ized* over time. Similarly in the operational result, the C2 system perceived a real world full of dangerous aircraft, but its internal structure very much shaped its interpretation in terms of what features to amplify and what types of actions to enable. Control loops are the basic building blocks of distributed cognition, but nevertheless, it's analytically useful to consider their "objective" and "subjective" aspects one at a time. The distinction between objective and subjective stability provides a basis for critiquing organizational policies.

---

[58] Overy, *Battle of Britain*, 34-6, 109

We will consider the external stability of air defense in three parts: the physical constraints on the problem; the consistency of British understanding of the problem through the interwar years; and the "cooperation" of the Germans in not complicating the problem as much as they might have. These are problems of clarifying whether perception and articulation cascades are even possible in principle given the technical state of the art and "dirtiness" of the battlefield. The challenge of achieving integration of the whole system will be deferred until the following discussion on the "subjective" side of British air defense, or internal consensus.

8.3.1 Physical Constraints

One reason that war is theoretically useful in the general study of organizations and technology is that it can check the tendency of some students of those fields to over-emphasize the social construction of everything.[59] Militaries confront real and dangerous structure in the world which costs them dearly if misunderstood. They thus seek to know the fixed and changeable constraints they face and to know the difference between them. Robert Brooke-Popham, the commander of RAF Air Defence of Great Britain (ADGB) prior to the creation of Fighter Command, observed that air defense "is not merely a problem of relative speeds but of absolute factors, some of which are invariable. The speed of the bombers is steadily increasing; on the other hand two other factors remain constant; firstly, the distance of London from the coast and secondly, the time that must elapse between the aircraft being seen by observers and the defending aeroplanes leaving the ground."[60] In 1933 Brooke-Popham was deeply concerned about the emerging inadequacy of existing air defenses against improving bomber capabilities, but he saw this in the context of some significant static constraints. Britain was an island and London's location was fixed upon it. Enemy bombers would have to cross the Channel to deliver their loads directly over their targets, and in doing so they would expose themselves to detection at some point. The only way to prevent the bombers from reaching their targets would be to put up some kind of barrier. Because it was infeasible build a wall in the sky, it would have to be a dynamic barrier that detected bombers and materialized in their path, whether in the form of fighters or artillery barrages. The allowable time between detection and interception

---

[59] Wiebe Bijker, Thomas P. Hughes and Trevor Pinch, eds., *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (Cambridge, MA: MIT Press, 1987); Ian Hacking, *The Social Construction of What?* (Cambridge MA: Harvard University Press., 1999)

[60] John Ferris, "Fighter Defence Before Fighter Command: The Rise of Strategic Air Defence in Great Britain, 1917-1934," *Journal of Military History* vol. 63, no. 4 (1999), 882

would vary with the speed of bombers and accuracy of interception. By no means did these constraints uniquely specify the air defense problem, just as the properties of grass, wind and muscle don't determine the rules of football. But they certainly did bound it, and clearly enough so that any changes in some of the basic constraints—the speed of bombers or the range of early warning detection—stood out against a stable background.

Throughout the description above we saw how representational operations exploited physical stabilities: the properties of electromagnetic energy and acoustics for aircraft detection, Chain Home Low's high-frequency "searchlight" to fill the low altitude gap, rate-time-distance constraints for aircraft track management, geometrical relationships for DF triangulation and the "Tizzy Angle," *etc.* Stable structure in the physical world constrained and enabled all representational cascades, and it was the ultimate referent with which they tried to coordinate.

Most importantly, the "ontology" of air defense was quite simple. There were few *types* of things in the real world to keep track of: airfields, radar stations, observer posts, fighters, bombers, and so forth. Aircraft tracks were basic unit of analysis, and there were few *properties* of import to describe them, such as speed, altitude, heading, number, friend-or-foe, *etc.* There were also few irrelevant types and properties to get in the way: airplanes flew through a mostly homogenous medium devoid of confounding barriers and human activity like on the ground. Weather created noise in detecting, but not new categorical types of things in the world. The *relationships* that mattered were largely spatial positions of aircraft in the sky and aircraft within sector territories or proximity to their targets, and such movement obeyed rate-time-distance and physical and electromagnetic constraints. The ontology was *durable*, which means that these types, properties and relationships were relatively stable: friends and enemies didn't switch sides, neutral pilots didn't have to be seduced or cajoled, airplanes didn't turn into ships, one airplane didn't break into two (although formations might split into sections) or teleport, and Fighter Command didn't have to track the Luftwafe's messy activities on the ground in France in realtime detail. This relatively simple and homogeneous world was ideally suited to representation, because a small set of discrete symbols could be arranged in a structural relationship which mapped rather straightforwardly onto the structure of the real world. Structural relationships among symbolic tokens in the space of the plotting room mapped straightforwardly onto structural relationships among airplanes in the sky. When an organization

is confronted with new emerging types and properties of things in the world to deal with, or large numbers of either to characterize and prioritize (like the SOTF with the counterinsurgency problem), then it is much harder to establish a discrete symbol set to represent these things in the real world, to say nothing of setting up the control channels to keep those symbols in coordination with the world. With a messy and changeable ontology, it's very hard to know when and if one has figured out which types, properties, and relationships among things matter for getting the job done, or how one's own "subjective" actions might alter the "objective" ontology, or what indeed is the right job to get done anyway.[61] Air defense, by contrast, is a pretty sweet problem for IT representation.

8.3.2 Learning the Right Lessons

The most important indication of the stability of the British air defense problem is that, with the important exception of radar early warning, the system in the Battle of Britain was amazingly similar in its basic contours to the London Air Defence Area (LADA) of the First World War. On that solid foundation, the RAF systematically worked out the details for an expanded system throughout the 1920s and 1930s. As bomber speeds increased, the "Channel gap"—the inability to detect aircraft far out over the English Channel—became a growing concern that could not be addressed until the emergence of radar in 1935. Nonetheless, the C2 fundamentals of track filtering and integrated information management had already been established and exercised before then.

Historian John Ferris argues that the ADGB "system was ideally preadapted to radar."[62] Signals intelligence, acoustic detection, British fighters of the day, and the integrative information system were well matched against early 1930s bomber technology: "Britain did not need radar to master the threat of 1934. Radar was essential for that of 1940, though far from sufficient for victory."[63] David Zimmerman's authoritative work on the development of British

---

[61] The frustratingly circular problems of epistemology rear themselves up right here. Messy ontologies prompt all sorts of chicken-and-egg questions about what's really in the world and what is brought forth through subjective cognitive and social construction. If the types of things in the world are more durable, then the subject-object distinction becomes more feasible. There's a reason that military personnel are pragmatically comfortable with the idea that there's an objective world "out there," since getting it wrong has lethal consequences.

[62] *Ibid*, 884

[63] *Ibid*, 881

radar strongly reinforces this revisionist interpretation.[64] The traditional narrative is that the RAF completely neglected air defense until Robert Watson-Watt invented radar and Hugh Dowding built an operational system around it. Ferris and Zimmerman, by contrast, pursue a core line of argument from the sociology of technology that the historical and institutional contexts of innovation explain more than the actions of a few great men.[65] In this case, the RAF was actually thinking seriously about air defense, even though its doctrinal preferences clearly favored offensive strategic bombing. We will temporarily postpone discussion of this serious doctrinal threat to consensus in order to first clarify how the RAF built air defense on its First World War foundations during the interwar years. In getting to know the essential contours of the air defense problem, the RAF created a favorable environment to foster radar development by the scientists.

This history of RAF experimentation and consolidation strays into "subjective" territory in that the RAF was building up its understanding of and consensus about solving the air defense problem. I include it here in the discussion of the "objective" problem in order to provide some historical basis for the stability of the problem. This is about whether or not it's possible to connect to and thus know the world in principle. The historical approach can reveal not only the stable features of the problem, but also show how the problem can be destabilized when the technical possibilities change. In this case, the "Channel gap" in context of increasing bomber speeds was quite destabilizing.

8.3.2.1 London Air Defense Area

The RAF was created in World War I because of the air defense problem, even though it would later try to justify its status as an independent service in terms of a strategic bombing role. The British government was outraged after German Gotha raids in June and July killed over 200 Londoners, and in August 1917 appointed E.B. Ashmore to command the London Air Defence Area (LADA) with expanded authority. Government attention to the air threat spurred the creation of the RAF as an independent air service on 1 April 1918.

---

[64] Zimmerman, *Britain's Shield*; *idem*, "Information and the Air Defence Revolution, 1917–40," *Journal of Strategic Studies* vol. 27, no. 2 (2004): 370 – 394.

[65] David E. Nye, *Technology Matters: Questions to Live With* (Cambridge, MA: MIT Press, 2006); Thomas P. Hughes, *Human-Built World: How to Think about Technology and Culture* (Chicago, IL: Univesity of Chicago Press, 2004)

LADA's C2 system was not fully up and running until September 1918, four months after the last major German attack, so it never really had a severe test, but its C2 should sound familiar. Signals intelligence provided warning of bomber launches (and tracked lumbering Zeppelins in flight) and visual observers provided adequate warning of slow-moving bombers. Dedicated telephone lines connected 25 regional sub-control rooms that plotted observation reports and used "tellers" to report back to LADA HQ. There a dozen plotters, connected via headphones to the sub-control rooms, updated a large map with "an ingenious system of colored counters" synchronized to a colored clock to keep the map from getting overcrowded. Ashmore took in the panoptic view from a raised dais where he had radios to the sub-control rooms at the aerodromes. Observer reports percolated up to LADA HQ in one minute and fighters were airborne in three to five minutes, which is a detection-to-interception timeline comparable to Fighter Command in 1940 (although the latter dealt with a far greater volume of raids across much greater distances). With a thousand people involved in the assessment and distribution of information, LADA could react to raids already underway, although articulation was the weakest link of the system in the absence of HF/DF or decent radio sets in the fighters.[66]

LADA was an important wartime innovation and early precedent for Fighter Command.[67] "E. B. Ashmore was the architect...Nothing essential started in 1936; rather it was a recovery that started. Dowding was the principal builder rather than the architect."[68]

8.3.2.2 Air Defense of Great Britain

LADA stood down after the war. While the RAF nurtured an enthusiasm for strategic bombing in the absence of any serious funding, it also grudgingly accepted a role for air defense. In 1924 the Joint Sub-Committee on the Air Defense of Great Britain described the "necessity...[of] a defensive system, combined with an active offensive."[69] In January 1925 the RAF thus formed ADGB with an operational sub-command called Fighting Area Headquarters (FAHQ). ADGB initially focused on an ostensible air threat from France. This fear receded by

---

[66] Neil Young, "British Home Air Defence Planning in the 1920s," *Journal of Strategic Studies* vol. 11, no. 4 (1988): 492-508; Zimmerman, *Britain's Shield*, 2-3 (the quote is from E.B. Ashmore); Ferris, "Fighter Defence Before Fighter Command," 853; John Ferris, "'Airbandit': C^3I and Strategic Air Defence during the First Battle of Britain, 1915-1918," in *Strategy and Intelligence: British Policy during the First World War*, eds. Michael Dockrill and David French (London: Hambledon, 1995)

[67] LADA is an interesting counterexample to Stephen Rosen's claim that wartime innovation is unlikely; *idem, Winning the Next War: Innovation and the Modern Military* (Ithaca, NY: Cornell University Press, 1991)

[68] Probert and Cox, *The Battle Re-Thought*, 56

[69] Ferris, "Fighter Defence Before Fighter Command," 857

the end of the decade and Germany took its place not long after. Ironically the Battle of Britain would be fought against Germans flying out of France, so this early orientation proved prescient. The fungibility of enemy identity also attests to the basically stable nature of the air defense problem vis-à-vis bombing London from the continent.[70]

ADGB organized an Ops Room like Ashmore's "to provide an intelligence centre upon which are focused all sources of intelligence" and to coordinate "the activities of all units of the defending force, both air and ground."[71] The Observer Corps was created in 1925 with four group headquarters and 100 posts, although ADGB did not get command over observers and coastal defenses until 1929; by then it had become clear that centralization was required to coordinate all the intelligence reporting. They recognized the need to maintain a separate intelligence plotting table at ADGB to filter the data before cluttering the Ops Room plot at FAHQ. A redundant network of landlines, including teleprinters, was laid in by 1934.[72]

This C2 articulated over a 15-mile deep "Aircraft Fighting Area" divided into eight sectors with Inner and Outer Artillery Zones which friendly fighters were to avoid. One weakness of this cordon system was the difficulty of concentrating fighters across sectors. Interceptions were guided from the ground, but not precisely, along a line of bearing where the bombers were expected. The entire Fighting Area was set 35 miles back from the coast to enable observers and acoustic sites to provide warning. This basic scheme remained in place until 1935 when bomber speeds started to cut too deeply into warning times.[73]

ADGB basically reconstituted and refined LADA's C2 and fighter squadrons from 1924 to 1930. It then undertook systematic improvement through exercises and research until it was replaced by Fighter Command in 1936 to reorganize air defense around radar. One of ADGB's most important achievements was the institutionalization of C2 information management.[74]

---

[70] Young, "British Home Air Defence Planning," 499

[71] Zimmerman, *Britain's Shield*, 40

[72] Wood and Dempster, *Narrow Margin*, 96; Young, "British Home Air Defence Planning," 501; Ferris, "Fighter Defence Before Fighter Command,"859-60

[73] Young, "British Home Air Defence Planning," 495-6; Ferris, "Fighter Defence Before Fighter Command," 857

[74] Ferris, "Fighter Defence Before Fighter Command," 863; Wood and Dempster, *Narrow Margin*, 44; Zimmerman, "Information and the Air Defence Revolution"

8.3.2.3 Acoustic Mirrors

The idea of a system of scientifically-designed sensors for early warning did not originate with radar. The War Office created the Acoustical Section of Signals Experimental Establishment in 1919 (renamed the Air Defence Experimental Establishment in 1925). W.S. Tucker, who had developed a microphone to direct counter-battery artillery fire in World War I, oversaw the office's 15-20 personnel working mostly on early warning projects. A pragmatic experimentalist, Tucker developed a series of concrete acoustic mirrors which focused sound on a microphone or a listener before a stethoscope. A key test in 1923 demonstrated that a twenty foot mirror could detect aircraft at 18 miles and register its bearing at 10 miles. In 1933 the Air Ministry approved the Thames Estuary system, which was to have two massive 200 ft. mirrors and eight 30 ft. mirrors all connected to a central plotting room. Land acquisition problems delayed construction until 1935. The Air Ministry halted the project the same year and cancelled it altogether in 1937 only because radar was showing far greater promise. From 1931 to 1936, however, acoustic mirrors were the only real alternative for tactical early warning, even though their performance varied radically with the weather, and bomber speeds were rendering them obsolete. Nevertheless, sixteen years of acoustic research and development did help to establish working relationships between scientists and the RAF, to set a precedent for a coastal system of early warning sensors, and to further reinforce the importance of centralized information management.[75]

Another option for early warning was signals intelligence. It was built into ADGB C2 and provided operational warning of launch and some tactical information. Due to its secrecy, most people didn't know about this intelligence, including radar scientists, which contributed to some negative evaluations of ADGB in the mid-1930s.[76] In any case, the Channel gap remained an unsolved and increasingly dangerous problem until radar.

8.3.2.4 Regular Exercises

It's a military commonplace that forces fight like they train, and this was certainly true of British air defense. Years of regular exercises and studies enabled ADGB to work out

---

[75] Zimmerman, *Britain's Shield*, 9-27; for interesting technical detail on the mirrors and on "tactile perception," see Raviv Ganchrow, "Perspectives on Sound-Space: The Story of Acoustic Defense," *Leonardo Music Journal* (December 2009): 71-75

[76] Ferris, "Fighter Defence Before Fighter Command," 870-872. I have seen little mention of the use of human agents to provide for operational early warning of bomber launches via radio, but it seems like this would not have been hard to arrange.

information management, DF employment, and defensive tactics. ADGB held the first of its annual summer air defense exercises in 1927. 84% of bombers were intercepted in 1928, although bomber pilots complained that the exercises were unrealistic (although they were surely less unrealistic than the RAF's fanciful claims about bombing accuracy). Every exercise between 1928 and 1933 experimented with radio DF, and every after-action report from 1931 to 1933 concluded that fighters must have a radio, even at the cost of climb and speed, and even though it caused concerns that sector and HQ might clash because of the centralizing potential (a recurring concern with the introduction of new IT).[77] By 1934, however, early warning had become the most vexing problem as improvements in bombers increased the speed, height, and area of defense. Fighter patrols were prohibitively expensive with the number that would be required to maintain a screen. The 40% interception rate of the 1934 exercise was especially worrisome.[78]

Following the 1934 exercise, a scientific officer at the Air Ministry named Albert Rowe searched through the Ministry's files and found 54 different concepts relating to air defense. Most were rather zany, including the suggestion of radio death rays which, fortuitously, happened to remind one of Watson-Watt's assistants about a report he had seen by some scientists, who were studying the ionosphere and had experienced radio interference caused by passing aircraft. The Air Ministry's Committee for the Scientific Survey of Air Defence, better known as the Tizard Committee after its chief scientist Henry Tizard, was created in December 1934 to investigate all sorts of curious ideas, not just radar. Air Ministry demand for better air defense and early warning in particular was palpable in 1934. The information problem was becoming decidedly unstable as long as it grew less and less possible to establish a connection with incoming bombers in time to articulate an interception.[79]

ADGB's exercises greatly clarified RAF understanding of air defense, which helped stabilize the overall problem, but also to highlight the gaping problem of early warning, which

---

[77] The Observer Corps could provide decent tracking, but there was no way to get the information to fighters. Medium frequency DF debuted in 1924 with a single beacon for aircraft to home in on. A prototype of HF/DF "pip-squeak" with a set of three DF stations emerged in 1935 with the support of the Tizard Committee; Zimmerman, *Britain's Shield*, 111.

[78] Young, "British Home Air Defence Planning," 502; Zimmerman, *Britain's Shield*, 41, 60; Wood and Dempster, *Narrow Margin*, 108; Ferris, "Fighter Defence Before Fighter Commad," 861-2

[79] Zimmerman, *Britain's Shield*, 45-48

destabilized a critical part of it. The importance of these exercises is captured in the Air Ministry official history of radar: "the air struggle was fought without any large deviation from the technique of raid reporting, and fighter control organization evolved for defence in air exercises before the war."[80]

8.3.2.5 Radar Experiments

British radar progressed from Watson-Watt's jury-rigged proof of concept to integrated operational readiness in an incredible five years. Because ADGB had primed the RAF to think about the entire air defense *system*, work on integrating radar into the system proceeded simultaneously along with the development of the revolutionary sensor itself. The very first document that used the term "RDF" did not actually delve into the details of the device, but instead considered how it would be integrated into Fighter Command operations.[81] The Air Ministry's decision in September 1935 to go ahead with five Chain Home stations for £200,000 was a huge gamble on an unproven technology that couldn't even find bearing or height yet, which indicates the intensity of desire to restabilize the air defense problem.[82]

1936 was a challenging year for the scientists at Bawdsey struggling to get radar to work reliably, but in the same year the RAF worked out many of the processes for managing radar data, even though that data didn't yet exist. Tizard organized a series of experiments at Biggin Hill with the object of guiding fighters from the ground to interception off a notional coastline. They simulated radar contacts with DF transmitters on bombers in order to exercise the Ops Room in constructing a track and vectoring an interceptor to meet it. Initial experiments involved straight and level targets, followed by planned turns, then feints at the bomber's discretion, and finally arbitrary changes in altitude as well. At each stage they worked out the necessary calculations, refinements, and fighter tactics to accommodate progressively more complicated couplings of internal and external structure. The "Tizzy Angle" was one of the local innovations to emerge through this systematic stabilization of C2 processes. As a result of this series of experiments, and on faith that Bawdsey would get its radars working, Dowding decided

---

[80] *Ibid*, 197

[81] Zimmerman, "Information and the Air Defence Revolution," 370

[82] Zimmerman, *Britain's Shield*, 89-90; £200,000 in 1935 is about $20.3 million adjusted to 2009.

to do away with the venerable concentric rings of the Aircraft Fighting Zone in order to instead vector fighters throughout the entire airspace.[83]

Technical progress at Bawdsey picked up considerably in 1937. With three Chain Home prototypes up and running, Bawdsey constructed a filter room to work out the specialized techniques. Testing through 1938 included radar countermeasures which led to the "long afterglow" CRT which could amplify the real signal in the flickering jamming. Chain Home and the Filter Room were ready for their first major test as part of the system in time for the 1938 summer exercises. This exercise revealed problems in processing a high volume of unpredictable raids, too many radar echoes, difficulties classifying tracks as friend or foe, trouble with teleprinters, and oversaturation of Filter Room with more than 141 tracks. With the radar chain now transferred to operational commanders, many of the Bawdsey scientists applied themselves with alacrity to addressing these problems in the first self-conscious and deliberate application of "operational research," about which more later.[84]

LADA established the basic concepts and organization of air defense. Throughout the interwar the RAF systematically refined and exercised these concepts in order to stabilize the problem, and in particular the multi-source information integration piece. As improvements in bomber technology threatened to destabilize the problem by undermining timely connection to raids, the determined demand for and development of radar solved the Channel gap crisis.[85] By the time the war got underway, the British had rigorously planned and exercised their defense. Fortunately for them, the Germans largely played along with their plan.

8.3.3 A Cooperative Enemy

War is finally a contest between adversaries. The enemy is ultimately the most important component of a military information problem. As an active willful combatant, the enemy tries to prevent friendly control loops from closing and is thereby a potent force for destabilizing the

---

[83] Neale, "CH," 82; Zimmerman, *Britain's Shield*, 109-115; Zimmerman, "Information and the Air Defence Revolution," 378-80; Wood and Dempster, *Narrow Margin*, 110-112

[84] Wood and Dempster, *Narrow Margin*, 85; Zimmerman, *Britain's Shield*, 161; M. Kirby and R. Capey, "The Air Defence of Great Britain, 1920-1940: An Operational Research Perspective," *Journal of the Operational Research Society* vol. 48, no. 6 (1997): 555-568

[85] Brett Holman, "The Widening Margin," *Airminded Blog* (27 May 2008), http://airminded.org/2008/05/27/the-widening-margin, presents an interesting set of quantitative estimates of the differing visual, acoustic, and radar warning times between 1914-1945. Holmon estimates that in 1939 these different means provided 5 min (visual), 10 min (acoustic, had it been constructed), and 40 min (radar) warning times to London.

information problem. The Germans did not realize this potential to the fullest effect during the Battle of Britain, however. The Luftwaffe made many mistakes—largely because it had to deal with its own considerable information friction—which contributed to the stability of British air defense.

8.3.3.1 Unprepared for a Strategic Offensive

The Luftwaffe got up and running only in 1935, but as we have seen, the RAF was taking material preparations well before that. The Luftwaffe used this time to prepare to support ground forces on the offensive, and it performed well in that role in Poland and France. However, there was no serious planning for nor operational concept of independent strategic air operations, to include gaining air superiority, nor did the Luftwaffe have any four engine bombers. One German general described Hitler and Göring's style as "romantic warfare," and indeed the Luftwaffe was expected to improvise a very ambitious campaign on little notice; the invasion was apparently suggested to Hitler by Admiral Raeder only in May 1940. The campaign furthermore had to be conducted from unfamiliar airfields in occupied France at the end of a long logistics chain, backed up by a discombobulated aircraft industry and supply system. The internal friction and lack of preparation was a major drag on Luftwaffe effectiveness.[86]

8.3.3.2 The Phony War Provided Training

Fighter Command was not as prepared in September 1939 when it declared war on Germany as it was in July 1940 when the Battle of Britain finally started. Chain Home Low was not yet up; many Chain Home stations were not well calibrated; not enough filterers had mastered their mysterious art; there remained some confusion about how much data to push down to the group level and vice versa; IFF wasn't working very well or installed in enough aircraft; and perhaps worst of all, fighter inventories were too low. After no serious German attacks materialized in the first six days of panic, Fighter Command stood down into a "normal" wartime routine and started debugging. Sporadic German patrols and insignificant raids over the next several months gave the entire system plenty of realistic practice. When the bad winter weather moved in, Fighter Command had a much clearer idea of what problems needed to be

[86] Boog, "Luftwaffe and the Battle of Britain," 18, 24; Overy, *Battle of Britain*, 18-19, 53-54

worked out. In the summer, furthermore, the pace of the battle picked up only gradually. The Luftwaffe couldn't have planned a better training regimen for Fighter Command.[87]

8.3.3.3 Intelligence Failures

Relationships between German intelligence and decision-makers were notoriously pathological. Given the poisonous internal politics of the Nazi regime, intelligence agencies were insular and loathe to share across boundaries; this fragmented Luftwaffe perception. Intelligence officers had low prestige and often just told their customers what they wanted to hear. Brimming with confidence after the sweeping victory over France, they woefully underestimated the RAF and were slow to realize their errors.[88]

The Luftwaffe's biggest intelligence failure was to not detect Chain Home before the battle; as a result they did not develop effective countermeasures. The Germans themselves had developed decent radar sets, and the Chief of Luftwaffe Signals suspected that the British might have as well. He sent the airship *Graf Zeppelin* on collection flights over the Channel to investigate the possibility, but it failed to recognize Chain Home even though the sky was literally full of its "floodlight" radiation. In a classic case of mirror imaging, the Germans assumed that any British radar would use short wavelengths like the German sets rather than the long 12 meter waves of Chain Home; the British were fortunate that Chain Home Low was not yet operating! The Germans dismissed the pervasive noise as an artifact of inefficient British communication (which meant they were doubly wrong). The Germans even captured a British set in France in May 1940, but apparently did little with it. Luftwaffe Signals certainly knew about Chain Home by late July, but the information wasn't well disseminated. At any rate, there was no determined German jamming until well into September; British operators were able to work through it, and by then it was too late to do much good anyway. [89]

While the Germans had radar, they did not yet have an integrated air defense system. Thus they also misunderstood how Fighter Command used radar. The Luftwaffe's July 1940 assessment of Fighter Command C2 missed the mark on almost every point:

---

[87] Zimmerman, *Britain's Shield*, 175-6

[88] Cox, "A Comparative Analysis of RAF and Luftwaffe Intelligence"

[89] Zimmerman, *Britain's Shield*, 204-7; Wood and Dempster, *Narrow Margin*, 68; Probert and Cox, *The Battle Re-Thought*, 69

> [RAF] command at high level [Fighter Command HQ] is inflexible in its organization and strategy. As formations are rigidly attached to their home bases, command at medium level [Group] suffers mainly from operations being controlled in most cases by officers no longer accustomed to flying (station commanders). Command at low level [Squadron] is generally energetic, but lacks tactical skill....the Luftewaffe is in a position to go over to decisive daylight operations owing to the inadequate air defense of the island....In the event of an intensification of air warfare the Luftwaffe, unlike the RAF, will be in a position in every respect to achieve a decisive effect.[90]

The Germans set up radio monitoring stations along the French coast in July, and they heard English voices calmly and systematically vectoring fighters over the ether. Even as it became clear that the RAF was using radar and vectoring fighters, the Luftwaffe interpreted this as evidence of C2 rigidity, which was another instance of mirror-imaging.[91] As late as 7 August Luftwaffe intelligence still assessed that "the British fighters are controlled from the ground by [radio, and thus] their forces are tied to their respective ground stations and are thereby restricted in mobility...Consequently the assembly of strong fighter forces at determined points and at short notice is not expected."[92] The Germans didn't understand the extent and flexibility of British ground control all the way up to visual engagement, so they underestimated the level of resistance their raids would meet. More importantly, they did not realize that they should have deliberately attacked British C2. [93]

8.3.3.4 Haphazard Targeting

Fighter Command's C2 system was both vital and vulnerable. Fortunately the Luftwaffe did not attack it systematically. In fact, "no target system, whether airfields, communications, ports or industry, was attacked repeatedly, systematically or accurately."[94] The Luftwaffe's diverse target catalogue lacked detail or unifying concepts. This was, in part, an artifact of the Luftwaffe's general confusion over what strategic aim it was trying to achieve at different moments of its improvised offensive: support for the Army's landing for Sealion, the defeat of

---

[90] Wood and Dempster, *Narrow Margin*, 67

[91] Many German pilots resisted the adoption of GCI during the defense against the Allied bombing campaign because they feared sacrificing control and flexibility; David Pritchard, *The Radar War: Germany's Pioneering Achievement 1904-45* (Wellingborough, U.K.: Patrick Stephens Ltd, 1989), 206.

[92] Wood and Dempster, *Narrow Margin*, 69

[93] *Ibid*, 116; Probert and Cox, *The Battle Re-Thought*, 58; Boog, "Luftwaffe and the Battle of Britain,"22; Cox, "A Comparative Analysis of RAF and Luftwaffe Intelligence," 436-7.

[94] Overy, *Battle of Britain*, 115

Fighter Command or other RAF commands, the destruction of all of RAF and its industry, disruption of the whole economic system, attacking British morale, or some combination thereof. Moreover, Luftwaffe targeteers were untrained in science or math, in contrast with the operational research approach that guided the Allied bombing campaign; therefore, targeting would have probably been haphazard even with clear strategic guidance.[95]

Targeting was particularly unfocused against Fighter Command C2. The Luftwaffe believed wrongly that all Ops Rooms were in hardened bunkers, so they didn't focus on them. Most of those critical nodes were actually unhardened, and yet sector Ops Rooms were only knocked offline three times (and quickly reconstituted). Chain Home stations with their unhardened huts were only attacked six times. The radars proved to be intimidating targets for German pilots because of their tall masts and wires, and the lattice towers weathered the blasts quite well when they were hit. Luftwaffe damage assessments were thrown off when Chain Home sites appeared to keep working even after being bombed (a result of either mobile replacements moving in to fill the gap or damaged sets that the British allowed to continue transmitting), so they concluded that the stations were too hard to damage.[96] Determined attacks probably could have blinded Fighter Command had they been pursued relentlessly.

Only in the last week of August was there anything like a systematic attack on 11 Group's infrastructure, the highest point of crisis for the air defense system. But instead of finishing the job, the Germans refocused their attacks on London in early September. Luftwaffe Field Marshall Kesselring was convinced—erroneously—that Fighter Command was largely destroyed and its fighters depleted. The combination of bad intelligence, German hubris, fickle targeting, and unrefined ideas about population bombing all came together in this most serious misstep in Luftwaffe decision-making during the Battle of Britain. With the pressure off, Fighter Command was then free to inflict serious damage on Luftwaffe bombers operating at the limit of their Me-109 escorts (which had been ordered to fly amongst the bomber formations, with the

---

[95] Boog, "Luftwaffe and the Battle of Britain," 23-24. This strategic confusion and haphazard targeting bears an uncanny resemblance to NATO's 1999 air campaign against Serbia. On the dubious effectiveness of operational research in Allied bombing see M. Kirby and R. Capey, "The Area Bombing of Germany in World War II: An Operational Research Perspective," *Journal of the Operational Research Society* vol. 48, no. 7 (1997): 661-677

[96] Wood, "Dowding System," 9; Wood and Dempster, *Narrow Margin*, 70; Boog, "Luftwaffe and the Battle of Britain," 26

intent of protecting bombers, but with the result of further undermining Me-109 performance advantages).

The Luftwaffe failed to reliably and consistently close the targeting loop on Fighter Command, while the RAF maintained its ability to close the loop on German aircraft.[97] The RAF's information problem was stable because the Luftwaffe's was not.

8.3.4 The Stability of Defense

To sum up so far, the RAF's information problem in the Battle of Britain was relatively stable. The LADA concept was basically sound given the physical contours of England's bombing threat and durable "ontology" of air defense. ADGB worked to deliberately improve it through the development of acoustic mirrors for early warning and annual exercises to test the system. When the Channel gap early warning crisis emerged because of improving bomber capabilities, it began to destablize the problem. The RAF then worked deliberately to stabilize the development and employment of new radar technology to fill the gap. By the beginning of the battle, the British were well prepared to manage a particular sort of information problem. The Germans then could have done a lot to destabilize this problem, but they had too many of their own self-inflicted information pathologies to deal with.

There is a larger question here about whether the information problems of defense are more stable than the offense. This would be an information-management version of the Clausewitzian dictum that defense is the stronger form of war.[98] Clausewitz argues that the attacker with the positive object of conquest must deal with greater political controversy and uncertainty than the defender, who has only the negative object of parrying the blow and surviving. The Luftwaffe had to develop and prioritize target sets and assess its campaign amidst ambiguous strategic guidance, while Fighter Command had relatively simpler categories of things it had to track and a clearer mission. The defender can trade space for time, allowing the attacker to make mistakes and become exhausted in an unfriendly environment; with the advantage of internal lines, the defender can shift forces around to meet breakthroughs. Interior lines provided the British with ownership over domestic communications, easy intermingling

---

[97] Overy, *Battle of Britain*

[98] Carl von Clausewitz, *On War* (Princeton, NJ: Princeton University Press, 1976), Book VI; Jon Tetsuro Sumida, *Decoding Clausewitz: A New Approach to On War* (Lawrence, KS: Kansas University Press, 2008), 153-175.

among scientists and military personnel to address emergent problems, and most importantly a thoroughly interconnected hierarchical C2 system with panoptic "centers of calculation." The defender, moreover, can rely on popular guerrilla resistance, which Clausewitz acknowledges is usually quite murderous. In the big picture, Fighter Command was not the last line of defense for England against Sealion, whereas the Luftwaffe *had* to win in order for Sealion to go ahead. It probably never had much hope of doing so in any case.[99]

I am not willing to go so far as to assert that defense is always a more stable information problem than offense,[100] although in this case that appears to be true. Fighter Command was more often than not able to connect with Luftwaffe raids: perception and articulation were possible in principle. Actual integration was not a historical given, however. We now turn to some of the political challenges that arose in implementing the solution described above.

8.4 Internal Consensus about Air Defense

The previous discussion of the external stability of the air defense problem inevitably included a great deal of "subjective" organizational effort to stabilize the problem. This is inevitable insofar as actors have no privileged outside perspective to get to know the world, and that knowing requires a lot of practical interaction and exercising. It is analytically useful, nonetheless, to be able to characterize the problem as externally stable and some solutions as better than others, so that we can see how internal politics might hobble the organization's ability to discover and implement effective solutions. If we do not make this distinction, then there is no real basis for critiquing policies. I relied on this distinction when I described the Luftwaffe's mistakes. Their offensive information problem was harder than the defense (because it involved targeting cycles with many different categories of things in the world to track and complex assessments to make), but it is quite clear that the Luftwaffe was internally dis-integrated in terms of solving it. They could have done better.

Likewise, the British could have done worse, and they almost did. We now take up some of the internal struggles that could have derailed the integration of British air defense. The big ones are the RAF's doctrinal bias toward the strategic offensive and politicized disagreements

---

[99] Robert Stanhope-Palmer, *Tank Trap 1940, or No Battle in Britain* (N. Devon, U.K.: Arthur Stockwell, 1976)

[100] Indeed, one of the reasons why military organizations generally prefer offensive doctrines is that it allows them to control uncertainty by choosing the plan of attack that supports their organizational processes while at the same time denying the defender his favored scenario; Posen, *Sources of Military Doctrine*, 47-48.

among scientists under conditions of technical uncertainty and government secrecy. Fortunately these conflicts were more or less resolved in time so that the RAF ended up with the integrated hierarchical "Dowding system" prior to hostilities.

8.4.1 RAF Strategic Bombing Doctrine

The traditional historiographic interpretation of the RAF is that it was so enamored with the idea of strategic bombing as an independent war-winning weapon that it neglected or even suppressed defensive doctrine. Air defense was thus ignored until radar and Dowding emerged with the backing of civilian politicians.[101] The first part is not inaccurate: most RAF officers believed strongly in offensive doctrine. The second part is misleading, however. As we have seen above, the RAF developed air defense and did so quite deliberately throughout the interwar years. While the RAF's expressed preference was for offense over defense, its behaviorally revealed preferences show acceptance for the possibility and preparation for the necessity of defense. Many historians have overstated the internal RAF doctrinal threat to consensus about air defense.

8.4.1.1 Expressed Preference for Offense

Military organizations tend to prefer offensive doctrines that enhance their wealth, autonomy, prestige, and enable them to take initiative against the enemy rather than cope with the uncertainty of reaction.[102] The RAF after World War I was a young, insecure service that hoped to win wars by flying over navies and armies and attacking the will of an enemy nation directly. The traumatic bombings of London—carried out before LADA was fully operational—reinforced an emerging zeitgeist of airplanes as unstoppable wonder weapons. Future wars would be moral conquests to discover which people could withstand the heaviest blow from above. Defensive airplanes—fighters—were seen as a waste of money because they were thought to be ineffective against bombers and because they would divert resources away from the almighty bomber. Hugh Trenchard, Chief of the Air Staff, was the most impassioned

---

[101] Williamson Murray, "British and German Air Doctrine Between the Wars," *Air University Review* (March-April 1980); Malcolm Smith, *British Air Strategy Between the Wars* (New York, NY: Oxford University Press, 1984); Tami Davis Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914–1945* (Princeton, NJ: Princeton University Press, 2002). The clearest argument for civilian intervention in the RAF as the cause for its reorientation toward defense is found in Posen, *Sources of Military Doctrine*, 141-178.

[102] Posen, *Sources of Military Doctrine*, 47-50; Jack L. Snyder, *The Ideology of the Offensive: Military Decision Making and the Disasters of 1914* (Ithaca, NY: Cornell University Press, 1989)

advocate of this view: "the aeroplane is not a defense against the aeroplane, but...as a weapon of attack, cannot be too highly estimated."[103] Future Prime Minister Stanley Baldwin dramatically summarized this extreme position in a famous speech in 1932:

> I think it is well also for the man in the street to realize that there is no power on earth that can protect him from being bombed, whatever people may tell him. The bomber will always get through...The only defence is in offence, which means that you have got to kill more women and children more quickly than the enemy if you want to save yourselves.[104]

Most RAF officers agreed that offense was the best form of defense. Even Dowding, soon to become the champion of Fighter Command, refused at first to fund radar when he first heard about Watson-Watt's idea in February 1935; he asked the Tizard Committee to consider research to improve "offensive methods" instead.[105]

However, this offensive mindedness did not translate into simple agreement about the impossibility of defense. Trenchard was a vocal zealot of a small minority who believed that air defense was impossible. Most officers entertained broader conceptions of air power that included some role for air defense. Thus the RAF had professional debates over whether bombers should fly in day or night, how important it was to gain air superiority, and thus whether bombers should target enemy airfields before "strategic" infrastructure. Furthermore, if the air war was to be a contest of civilian will to endure bombing, then the civilians would need to be protected, for morale if nothing else, especially for a city like London so close to the ostensible French threat. Consideration of offensive doctrines naturally led to thoughts about air defense. Mention of strategic bombing took on a higher profile in the professional discourse because, ironically enough, there was more general agreement on the desirability of defense. If it was possible, then it was necessary, and so there was less to talk about.[106]

8.4.1.2 Revealed Preference for Defense

The Air Staff recognized a role for defense early on, if only grudgingly and if only to stiffen civilian morale. A 1922 Air Staff report recommended "a local defense force" to reassure

---

[103] Young, "British Home Air Defence Planning," 493

[104] Stanley Baldwin speech in Parliament, *The Times* (11 November 1932): 7

[105] *Ibid*, 56

[106] Ferris, "Fighter Defence Before Fighter Command," 848-851; Biddle, *Rhetoric and Reality in Air Warfare*, emphasizes Trenchard's zealotry, if not the existence of alternative defensive currents in the RAF.

civilians with an aircraft defensive zone around London. The concept was further fleshed out in a 1923 report from a subcommittee of a Joint Air Ministry and War Office Committee on Anti-Aircraft Defence, chaired by Trenchard no less, which defined the Aircraft Fighting Zone scheme adopted by ADGB until 1935. The RAF accepted that defense, in addition to offense and deterrence-through-offense, was part of its mission.[107] The stated principle of 1924 that "the bombing squadrons should be as numerous as possible and the fighters as few as popular opinion and the necessity for defending vital objectives permit" should be taken to mean that the RAF absolutely wanted defense first.[108]

The procurement behavior of the RAF provides strong evidence of its commitment to defense. In 1923 the RAF ultimately agreed to a Home Defence Air Force plan to field twice as many fighters and 20% fewer bombers than Trenchard wanted. By 1928, 14 of the total 52 squadrons (168 or 28% of the RAF's total aircraft) were to be fighters deployed in the Aircraft Fighting Zone. The Home Defence scheme was postponed seven years after the Treaty of Locarno in 1925; as it turned out, 1928 was the first year the RAF actually had barely more bombers than fighters, even though the original plan had been for a two-to-one ratio by then. In 1934 the ratio was still a comparable 12 fighter to 15 bomber squadrons. Between 1924 and 1931, every combat characteristic except firepower for RAF fighters improved 50-100%, and the Air Staff decided in 1934 to arm its future fighters with eight instead of two guns to address that gap. Moreover, the RAF allowed for a third of its bomber pilots to be reservists while all fighter pilots were supposed to be active duty because they required greater tactical skill. All of these developments during the lean years prior to rearmament indicate that fighters were not as far out of the RAF mainstream as commonly assumed. When taken together with ADGB's achievements, the "RAF could have not done much better had it explicitly aimed for defence rather than offence."[109]

Another discrepancy between the stated and revealed priorities of the RAF was in the application of science and technology. Axioms about strategic bombing were matters of deep faith for the Air Staff, so there was little effort to rigorously test them. When bombing tests were

---

[107] Young, "British Home Air Defence Planning," 494-496

[108] Ferris, "Fighter Defence Before Fighter Command," 852

[109] *Ibid.*, 852, 862, 865-6, 883 (quote); Young, "British Home Air Defence Planning," 498; Wood and Dempster, *Narrow Margin*, 57

finally conducted in 1937, they suggested that RAF bombers did not perform well, but Bomber Command hotly disputed the results.[110] It would later pay the price for its failure to learn during the early part of the Allied bombing campaign. By contrast, we have seen how ADGB and then Fighter Command regularly and systematically exercised and improved their technology and tactics. While scientific "operational research" examined and debugged organizational and technical processes for air defense, Bomber Command remained relatively uninterested in such assistance until summer 1941.[111] One might make the argument that it was *because* of the subordinate position of defense on the RAF totem that ADGB was actually free to proceed in a rational systematic fashion; there were no sacred cows to attack, and this marginal air defense community could thus develop as it wanted (much as MacArthur's Far East Air Force pioneered innovative doctrine outside of the mainstream U.S. Army Air Force ideological center of mass). Certainly there was no competition for the scientists' expertise from Bomber Command. While RAF leadership was enamored with strategic bombing, ADGB rationally explored what actually worked for air defense.

8.4.1.3 Rearmament Debate

The best evidence for the RAF's commitment to strategic bombing at the expense of defense is the acrimonious debate over rearmament in 1937-38. It's important to appreciate that *every* part of the RAF was materially unready in the mid 1930s. At last the money spigots were turning open, and bomber zealots who dominated the Air Ministry were eager to drink up. At the same time the Chamberlain government was terrified of German bombing (apparently they had listened to the RAF about the devastation of air power) and outraged about the weaknesses of Bomber Command that were then being exposed. Fighter Command showed promise, meanwhile, and fighters were certainly cheaper per unit than bombers. RAF rearmament planning dragged out through many iterations over disputes on the proper fighter/bomber mix until Scheme M with a fighter emphasis was finally adopted on 7 November 1938.[112]

The public offense-defense debate was real, as was the RAF's offensive bias. The debate was hindered, however, by the secrecy of radar. Many participants simply didn't understand just

---

[110] Paul Bracken, "Unintended Consequences of Strategic Gaming," *Simulation Gaming* vol. 8, no. 3 (1977): 310-312; Ferris, "Fighter Defence Before Fighter Command," 848

[111] Kirby and Capey, "The Air Defence of Great Britain," 565

[112] Smith, *British Air Strategy Between the Wars*, 198-226

how effective Fighter Command's system had become, so how were they now to make sense of years of public RAF ideological attacks on defense in favor of strategic bombing? Senior Air Ministry officials in the know could no longer argue that air defense was impossible, only that it was preferable to create a strategic deterrent through the ability take the fight to the enemy. Likewise, advocates for more fighters could not come out and say why air defense was now more reliable. Air Minister Lord Swinton, a public advocate of the Air Ministry's position on buying more bombers, resigned over the air rearmament controversy, and yet he had been a key protector of the Tizard Committee and later observed that "as soon as radar was discovered and proved, the theory that the only defense was counter-attack was dead." [113] Several like Swinton who were pilloried for not doing enough to secure the nation from attack were not at liberty to reveal how much they had been doing.

The debate highlights the complexity of the RAF's views on air defense. Chain Home was already approved, and "lower level internal memoranda reveal near unanimity of opinion in the Air Ministry and in the cabinet about the influence of the new technology."[114] The RAF wanted air defense, but it also really wanted bombers.[115] The debate over the pace of rearmament was muddied by the secrecy of radar, and it took much bitter negotiation by the civilian cabinet to finally push through a plan that built the fighters Dowding so desperately needed.

The negative impact on air defense of the RAF's offensive bias has been exaggerated in the historiography of British air doctrine. The RAF invested in air defense prior to the emergence of Dowding and radar onto the scene, most importantly in the critical area of C2. There was more consensus about its possibility and desirability than generally appreciated. In fact, the general consensus about air defense meant that it received much less public and professional discussion than the heady ideology of strategic bombing. The former proceeded

---

[113] Zimmerman, *Britain's Shield*, 134. Interestingly, Chain Home was kept secret even though it featured thirty-six extremely conspicuous radar stations. The government informed news organizations that the towers were being built for the air defense of Great Britain and asked them not to report on them. The press respected the request, a testament to an era of much healthier relations between the government and the fourth estate.

[114] *Ibid*, 134

[115] C. P. Snow, *Science and Government* (Cambridge, MA: Harvard University Press, 1961), describes the receptivity of the RAF to Tizard's activity "to persuade the serving officers of the Air Staff that radar was their one hope and, in general, to make scientists and military people understand each other. Here again this might have been impossible. In fact, with the exception of those concerned with bombing policy, the senior officers were ready to be convinced as soon as Tizard started to talk."

rationally without fanfare while the latter was dramatically flaunted without any bother of experiment. The doctrinal controversy did indeed threaten Fighter Command by delaying fighter procurement, but it would have been a whole lot worse had the sound foundations of air defense C2 not already been developed in the decades before. Civilian intervention dispatched this residual threat to consensus in time to make a difference, but in light of recent reinterpretations of radar history, the magnitude of doctrinal dissensus appears to have been overstated.[116]

8.4.2 Politicized Science

While orthodox strategic bombing doctrine held air defense in low esteem, the RAF nevertheless was receptive to the advent of radar because it had allowed ADGB to prepare the way. Yet another threat to consensus about how to implement air defense emerged among civilian scientists over the technical feasibility of radar. Frederick Lindemann's infamous dispute with Henry Tizard is a rather sordid example of how scientific research agendas are subject to politicization when the results matter for policy and power, especially when official secrecy complicates the evaluation of scientific knowledge.[117] This quarrel came closer to derailing radar research or compromising its existence to the Germans than anything else, either of which would have been disastrous for 1940.

Tizard was a critical player in the development of radar. Neither theorist nor experimentalist, he was a talented administrator, an increasingly important role in twentieth century techno-science. With his military background (Tizard flew fighters in the First World War) and "Establishment" credibility,[118] he forged close working relationships between RAF officers and scientists, ultimately swearing to secrecy more than 90 academic scientists to work on radar. The Tizard Committee investigated not only radar but a lot of other ideas which

---

[116] Posen's (*Sources of Military Doctrine*) theory of civilian intervention to cause innovative doctrine is a proxy mechanism for the influence of the international balance of power, contrasted with internal military preferences. While outside civilian intervention is not the whole story here—the RAF creates ADGB and Churchill's bluster almost undermines radar research—the larger story of international structure appears to be important. The threat is salient and existential and the information problem is stable, and it seems to affect RAF behavior in spite of its doctrinal preferences for strategic bombing. Civilian intervention is not the only mechanism by which the balance of power might prompt innovation.

[117] Sheila Jasanoff, "Contested Boundaries in Policy-Relevant Science," *Social Studies of Science* vol. 17, no. 2 (1987): 195-230

[118] C. P. Snow, *Science and Government*, writes that "everything went through with the smoothness, the lack of friction, and the effortless speed which can only happen in England when the Establishment is behind one. Within a very short time the Tizard Committee were asking for millions of pounds, and getting it without a blink of an eye." See also P. M. S. Blackett, "Tizard and the Science of War," *Nature* vol. 185, no. 4714 (1960): 647–653

eventually bore fruit later in the war: the proximity fuse, air-intercept radar, anti-radar chaff, anti-tank rockets, more effective balloon barrages, and so forth. Tizard enabled Watson-Watt's team at Bawdsey to conduct a wide range of experiments to operationalize radar, while also developing the techniques to use radar data.[119]

If Tizard is the long-suffering champion of scientific method in this morality tale, then Lindemann is the politically-connected jealous rival. Denied entry into the British military because of his German background, Lindemann became interested in applying science to aircraft detection during the First World War and later joined the faculty at Oxford. As a member of the interwar Anti-Aircraft Research Committee in 1925, he tried to undermine Tucker's acoustic mirrors, apparently misunderstanding the principles on which they were based. A decade later the eccentric physicist formed an enduring friendship with Winston Churchill, at the time a back-bench MP. Lindemann's obsession with air defense dovetailed with Churchill's obsession with the cause of rearmament to deter Germany (and to flog Prime Minister Baldwin).[120]

Churchill had already proved himself willing to use classified intelligence to make his points about rearmament in Parliament, so the stage was set for fireworks over radar in early 1935. Lindemann believed, with some justification, that the offense-minded Air Ministry wasn't taking air defense seriously. He also doubted the efficacy of the newly-created committee under Tizard, with whom he had a long and not always smooth personal acquaintance. In the grandstanding which followed, Churchill publically revealed the existence of the Tizard Committee, but not any specific projects. The outcome was a new rubber-stamp body for Churchill called the Air Defence Research Committee (ARDC) under the Committee for Imperial Defence, effectively duplicating the Tizard Committee, and membership for Lindemann on the Tizard Committee.[121]

A year later Lindemann was complaining again to Churchill that they weren't taking his ideas for aerial mines and infrared aircraft detection seriously. The latter was developed with some merit by Lindemann's talented student R.V. Jones later in the war, but his ideas about mile long wires, parachutes, balloons, and raining curtains of bomblets were half-baked. The RAF

---

[119] Kirby and Capey, "Air Defence of Great Britain," 560-561; Zimmerman, *Britain's Shield*, 49-51, 144-150
[120] Zimmerman, *Britain's Shield*, 6-7, 16-19
[121] *Ibid*, 37-39, 67-77

did, in fact, look at a lot of wacky schemes but couldn't get them to work. Lindemann prevailed on Watson-Watt, who happened to be in a petty spat with the Air Ministry over his pay and title at the time, to tell Churchill that there were troubles in the Tizard Committee. When Tizard pushed back, Lindemann announced his decision to run for Oxford MP to push his views. Tizard folded and the indispensable scientists P.M.S. Blackett and A.V. Hill resigned from the committee. Air Minister Lord Swinton, the titular head of the Tizard Committee, abruptly dissolved the committee, only to reconstitute it days later with Blacket and Hill; in place of Lindemann, who was not informed, they brought on E.V. Appleton, an expert on radio waves. Swinton's great fear was that radar would be compromised just as it was starting to bear fruit in 1936.[122]

The final round was launched during Churchill's withering attack on the Air Ministry for not rearming fast enough, which resulted in Lord Swinton's resignation in 1939. Egged on by Lindemann, Churchill again attacked the state of research and threatened again to publically reveal radar: "After nearly four years we have not been given any definite results. The story is lamentable, and only the public interest prevents it being told in Parliament."[123] Indeed, radar was the only innovative Tizard Committee project to pan out so far and Britain was still vulnerable at night (to be discussed later), but again secrecy undermined the evaluation of knowledge.[124] The outcome was that Lindemann joined the ARDC, which then stopped having regular meetings, effectively depriving Churchill of the insight into air defense he sought. Tizard was deeply shaken with the sense that the government had lost confidence in him. Lindemann was only finally muzzled when he was given an opportunity to test some aerial mine concepts, which failed, and Churchill was briefed on the full extent of radar, which greatly impressed him.[125]

If Lindemann had succeeded in wresting control of the air defense research agenda from Tizard, then the outcome for radar—and thus for the Battle of Britain—would have been

---

[122] *Ibid*, 93-108
[123] *Ibid*, 141
[124] C.P. Snow, *Science and Government*, wrote, "It is one of the classical cases of 'closed' politics coexisting with 'open' politics. Passing from one to the other, an observer would not have known that he was dealing with the same set of facts." The great irony is that the "Establishment" which Churchill attacked for dragging its heels and not rearming fast enough was in fact protecting the development of a revolutionary new technology.
[125] Zimmerman, *Britain's Shield*, 136-141, 151

calamitous. Churchill's interventions were launched with good intentions to improve air defense, but his scientific advice was way off the mark. Neither of the pair had all the relevant facts because of radar's secrecy, and this also hobbled radar's defenders in public debate. The experiments at Bawdsey did not just happen all by themselves, but they required active defense by Tizard from their political opponents. Fortunately Tizard prevailed and preserved the incubatory space that radar science needed.

Lindemann would cause no more problems for the Battle of Britain, although "the Prof's" dubious franchise was revived again after the battle when Lindemann became Lord Cherwell, science advisor to Prime Minister Churchill. In 1942 Tizard would challenge Cherwell's advocacy for area bombing of Germany and his inflated bomb damage assessments, but Cherwell carried the day. Cherwell's last significant contribution to British air defense would be to doubt the existence of the German V weapons which were to rain down on London in 1944.[126]

8.4.3 Fighters in France

A minor threat to consensus on Fighter Command's disposition materialized during the Battle of France. The RAF deployed fighters to support the British Army, but without prepared bases and radar guidance their losses were high (477 machines shot down in May and June). In a critical 15 May meeting Dowding used data prepared by his operational research scientists to argue that fighter wastage rates in France were unsustainable and no more should be diverted there. OR—a critical new information technology developed for Fighter Command—provided the rhetorical punch needed to drive Dowding's point successfully and re-establish his claim to Fighter Command's precious resources.[127] Dowding later reflected, "I am profoundly convinced that this was one of the great turning points of the war."[128]

8.4.4 The Dowding System

The air defense information problem was relatively stable. The RAF took the time to understand what was required to solve it, even though it was not in the prestige center of their doctrinal identity. The radar scientists were protected from adverse political influence so they could develop the technology which would stabilize the Channel gap problem. Dowding controlled his fighters.

---

[126] *Ibid.*, 230-232; Thomas Wilson, *Churchill and the Prof* (London, U.K.: Cassell, 1995)
[127] Overy, *Battle of Britain*, 8; Kirby and Capey, "Air Defence of Great Britain," 563-564
[128] Dowding, "Despatch," 4545

In fact, Dowding controlled nearly everything in Fighter Command. He was a micromanager who was into everything and had a firm understanding of how the whole system came together. There was "unity of command" in British air defense. This was reflected in the hierarchical architecture of the system, with all information feeding into the Ops Room at the apex of all perception and articulation cascades, and Dowding's official position as "Commander in Chief" of Fighter Command. It was also reflected in the common purpose that Dowding infused into all the diverse functional parts and tens of thousands of people who made up "the Dowding System." Vertical integration of the organization under Dowding's leadership imposed a further degree of consensus on its parts.

8.5 Expedient Adaptation of the System

Information friction theory describes three conditions for successful C2. We have seen how the British system met the first two of these with a relatively stable information problem and a rough consensus about the solution. When the information system enjoys both external stability and internal consensus, then the organization can close control loops on the enemy. When either condition is not met, then personnel have to struggle with a representational architecture that is uncoordinated with the structure of the world.

During wartime, it is inevitable that these two conditions will weaken somewhat, and thus the third is that the information system must be able to compensate. The enemy usually undermines "objective" conditions and internal pathologies stress "subjective" consensus. War is a contest of control, so both sides cannot be equally good at closing control loops. Moreover, each adversary continually "votes" to continue the war because they think they have a good chance of closing their own loops and winning the fight. Because information friction is inevitable during war, the organization must be able work through it in real-time. Specifically, it must be able to lower the barriers between technical expertise and operational knowledge needs in order to reconfigure the sociotechnical information system in the midst of wartime operations. *Expedient adaptation* essentially reestablishes the first two conditions during wartime. The result is often messy, self-organized, and just functional enough to get by. But it's better than the alternative, defeat.

Fighter Command experienced both varietals of information friction, mutual interference and bureaucratic insulation, but mostly the first. The first is failure to coordinate with a

destabilized problem. The second is excessive consensus that is inappropriate to the problem. Fortunately, Fighter Command also had the capacity to make corrections on the fly. "Operational research" was particularly important for joining technical expertise to operational needs in wartime. Instances of both types of information friction as well as of runtime design have been mentioned in passages above, but this section will explicitly draw them out.

8.5.1 Interference

Mutual interference occurs when the organization is unable to coordinate distributed processes. The actions of one component cause negative and unexpected consequences for another. Local initiatives for private gain degrade public welfare. The implementations of abstractions overflow or "leak"; black boxes malfunction.

8.5.1.1 Enemy Action

The enemy often alters aspects of the expected information problem and causes friction by breaking C2 components. The fall of France changed the approach and warning geometry insofar as the British had been worried about Germany invading from the North Sea. This was mitigated somewhat by prior 1920s planning for air raids from France. The proximity of French airfields to the coast complicated height estimates via radar because Luftwaffe formations were usually still climbing when they were detected, which exacerbated Chain Home's tendency to underestimate height. Some Luftwaffe tactics were not expected, most surprisingly the accompaniment of fighter escort along with bombing raids; British exercises had focused on intercepting just bombers. Counting the numbers of aircraft in a raid was one of the hardest measurements for radar operators; this was made even more difficult by the Luftwaffe tactic of vertically stacking fighters and bombers, because radar operators often assumed there was only one aircraft even they saw multiple height returns. Diversionary tactics, where Luftwaffe aircraft would break off at the last minute, were not unexpected because the RAF had exercised them before the war, but they still demanded careful concentration by plotters and controllers. Lastly, the physical destruction of infrastructure degraded C2. When the three sector Ops Rooms were bombed, their emergency relocations proved too cramped and insufficiently connected to landline telephones. Observation posts found themselves victims of strafing and bomb attacks,

and six radar stations were bombed. As we have seen, C2 attacks could have been far more paralyzing had the Luftwaffe focused harder on this target set.[129]

8.5.1.2 Radar Blues

The five year invention to operational integration timeline of radar development was remarkable, but it also meant that there were still a lot of bugs in the system at show time. No Chain Home station conformed to a standard design. Each one required individual calibration based on local landforms, weather patterns, and the vintage of its equipment. Calibration was a complicated matter requiring over 400 different observations and dedicated support flights, which were also tasked to train radar and filter operators at Bawdsey or grounded by bad weather. Many stations were still poorly calibrated by summer 1940. The continuous expansion of the chain—from 54 to 76 stations between 1 July and 30 September—complicated calibration of the sites and integration of the system. Continual upgrades took individual stations offline. Local efforts to improve station performance sometimes interfered with other stations. For example, each station was allocated a specific area on the 50 Hz waveform and not allowed to deviate without headquarters permission; nonetheless, they often did in order to deal with local ionospheric scattering, but by doing so, they inadvertently degraded the signal quality of neighboring stations. The idiosyncrasies of local stations often did not conform to the standardized station abstraction the centralized system expected.[130]

The skill of radar personnel also varied. The rapid expansion of the chain created a high demand for operators, and the abilities of the new recruits sometimes were not up to par. One scientist noted that even though radar sets were improving between 1939 and 1940, operator performance was degrading. Filtering became more difficult with the introduction of Chain Home Low, which had different imaging characteristics than Chain Home; it was only in May that the 36 Chain Home Low stations were online after the introduction of the first one in November, so there was little time to figure it out. Variable operator skill had consequences for the referential integrity of track plots. When IFF systems malfunctioned or operators couldn't read them, they usually assumed they were hostile. Height measurements were regularly underestimated, which placed fighters in a tactically disadvantageous position for interception.

---

[129] Wood and Dempster, *Narrow Margin*, 45; Zimmerman, *Britain's Shield*, 198-199, 201, 207; Overy, *Battle of Britain*, 79

[130] Zimmerman, *Britian's Shield*, 160, 190; Neale, "CH," 80

Controllers and pilots thus each tended to add a few angels (1,000 feet) to the estimate. Once radar and operator skill had improved, this habit had the effect of placing fighters too high to do any good! The problem of declining operator skill with Chain Home expansion was not solved until the RAF started relying heavily on the WAAF and raising performance standards.[131]

The most tragic form of information interference is fratricide. An illustrative episode of the interference hazards of radar is the bizarre "Battle of Barking Creek" on 6 September 1939. A friendly aircraft approaching from the direction of France had failed to file a flight plan. Chain Home operators did not get an IFF reading so they classified it as hostile and Hurricanes were sent to intercept. Inexperienced Chain Home operators confused the reciprocal bearing of the outgoing fighters while IFF failed again, so they classified them as a second incoming raid. Another squadron of Hurricanes was scrambled, and these were also classified as incoming hostiles, compounded by observer post misidentifications. After several iterations, there were eventually twenty unidentified "X" tracks in the Filter Room, prompting the launch of a Spitfire squadron, which eventually opened fire on what the pilots thought were Me-109s. Spitfires shot down two Hurricanes, and anti-aircraft artillery downed one Spitfire. In this case positive feedback went out of control, compounding local error upon error with tragic results.[132] In another case, a friendly Ansen filed a flight plan at 5,000 feet, but two Chain Home stations this time *over*estimated the height as 7,000 and 18,000 feet, respectively; the contact was designated a hostile track operating over 10,000 feet (assuming the normal tendency of radar to *under*estimate), but fortunately the fighters sent to intercept were able to visually recognize the friendly Ansen before they opened fire.[133] Both of these integration failures were finally perceived as breakdowns only when personnel were suddenly confronted with graphic information that was at odds with their symbolic track data: with the revelation of friendly fire, it became painfully clear that the state of the representation was uncoordinated with the state of the world.

Idiosyncrasies in the local transductions of radar contacts into symbolic data could undermine the referential integrity of the latter. The representational transformations became unconstrained, and the results thus uncoordinated with the structure of the world. Equipment

---

[131] Zimmerman, *Britian's Shield*, 167-8, 183-5, 188; Wood and Dempster, *Narrow Margin*, 118, 258
[132] Beyerchen, "From Radio to Radar," 285-6; Zimmerman, *Britain's Shield*, 175
[133] Zimmerman, *Britain's Shield*, 180

misbehavior and operator gaffs introduced noise into the radar information channel, but such equivocation was not always obvious in the neat discrete symbolic tracks that emerged from the "black box" radar station or Filter Room. Dowding noted that "the training of the technical personnel and the maintenance of the elaborate scientific apparatus presented great difficulties."[134]

8.5.1.3 Non-Observed

The Observer Corps channel was noisy also. Visual observation was defeated by low clouds, rain, and night. Height estimation was an acquired skill, and estimates were likely to be especially off if there was no time or ability to compare with neighboring posts. Height errors became position errors on the observer's sextant, which created zigzagging and misleading tracks at the observer center plots. Posts could be overwhelmed by too many aircraft, and observer center plots became cluttered. Many aircraft were misidentified as hostile because the Observer Corps was worried that otherwise their tracks would be ignored. Confronted with too many bad observer tracks cluttering up the Ops Room plot early in the war, Dowding ordered that only radar could be used to identify tracks, which could then be tracked inland by the observers. This resulted in some raids, missed by radar but not by observers, never being tracked.[135]

8.5.2 Insulation

Mutual interference patterns of information friction are distinguished by an experience of breakdown. The organization is unable to close the loop on the enemy. Insulation, by contrast, is premature closure on things other than the enemy. The system is *not* experienced as "being broken" by participants, even though it is actually having real troubles coordinating with the features of the world that really matter. As everywhere with these complex control systems, insulation at one level or for one group might be experienced as interference at another, and the distinction between them can be as fuzzy as the "objective" and "subjective" conditions for which these are the failure modes. For example, the "Barking Creek" fratricide surely had insular characteristics for a spell: the "centers of calculation" created their own skewed reality until it suddenly became tragically obvious that Fighter Command had just killed its own. The intuitive distinction between the two is that interference results from uncoordinated

---

[134] Dowding, "Despatch," 4546

[135] Wood and Dempster, *Narrow Margin*, 105; Zimmerman, *Britain's Shield*, 173

decentralization while insulation results from too much centralization. An information problem can be either unsolved or oversolved.

Insulation problems were not as pronounced for Fighter Command as interference issues. This is largely a consequence of the relative simplicity of the world it needed to track and the tangible feedback of non-intercepted raids which enabled self-correction. Insulation is most likely when an organization measures its own activity rather than its effect on the enemy; the clarity of feedback made this unlikely for Fighter Command. But even more, the low incidence of insular failures is a testament to the success of consensus-building about the solution during the interwar years; the RAF actually managed to come up with a solution that matched the problem the Germans would pose for it. In a counterfactual world where RAF strategic bombing doctrine maintained an iron grip on the organization and no preparations were ever made for defense, then we would certainly be witnessing a case of severe insularity.

Nevertheless, there were problems. Over-centralization clogged up the the C2 system, which was vulnerable to saturation at its integrative nodes. Preparation for solving the problem of daytime air defense left Fighter Command unprepared for the Night Blitz on London. Both of these were indeed perceived as breakdowns and thus also look a little like interference, but for the sake of illustration we can treat them as problems of too much consensus.

8.5.2.1 Saturation

The C2 system was vulnerable to information overload. Filterers and plotters were sometimes simply unable to keep up with the high volume of contact reports, and as a result the single air picture might have missing and bad tracks; there would be no way to know from the vantage of the Ops Room gallery. Sometimes the radar stations were ordered to stop reporting because the Filter Room couldn't deal with what it already had. An operational research report from November concluded that 5 filterers and 3 tellers at the single Filter Room servicing all three groups was insufficient; 11 Group alone should have had 7 filterers and 3 tellers just to handle the tracks over its territory.[136] The Air Staff pressured Dowding to decentralize by establishing Filter Rooms at the group level also, as well as providing greater autonomy to sector commanders. Ever the micromanager, Dowding sought to maintain control of a single air picture at Bentley Priory, lest squadrons scramble prematurely before it could be verified that a track

[136] Zimmerman, *Britain's Shield*, 202

was indeed a hostile raid bound for their sector. Given the premium on husbanding fighters, this was reasonable. Dowding's concession to a confrontation with the Air Staff in January 1940 was to move his Filter Room to an underground bunker to protect it and to "tell" tracks to the groups directly from the Filter Room. The saturation problem did not go away, however, and in fact became far worse once the real battle got rolling. On 1 October the Air Staff directly ordered Dowding to decentralize, and so a Filter Room was built at each of the group HQs to process radar data from stations in their territories. It's an interesting wrinkle that it required hegemonic authority to force a decentralized work-around of a problem of over-centralization.[137]

8.5.2.2 Night Blitz

Fighter Command's system performed admirably against the Luftwaffe during daylight attacks, but it was unable to deal effectively with the night raids that began in earnest in mid-September. Of the 6,135 Luftwaffe night sorties over Britain that month, the RAF only shot down four aircraft. Night intercept was harder for three reasons. First, they needed to have a larger two-crew aircraft to fit and to operate navigation apparatus, as well as more powerful canons for fleeting encounters with the enemy. The Bristol Blenheim, an adapted light bomber, proved barely mediocre in this role. Second, the intercept needed ground controlled intercept (GCI) with a radar that could closely track the target and the interceptor overland, rather than broad-search early-warning at sea. The PPI display was invaluable for GCI. Third and most important, the aircraft needed airborne intercept (AI) radar to close the gap between the 20,000 ft. limit of GCI and 500 ft. visual acquisition. Searchlights were defeated by high altitude because of the sound lag, so GCI and AI were the only intercept options.[138]

Tizard recognized the system's nighttime vulnerability as early as 1936. Indeed, it was one of Lindemann's foremost and legitimate complaints in their quarrel. AI was quite simply a hard problem, as the transmitter and receiver had to be quite compact, and as ground clutter swamped the display for targets closer than 1,000 ft. While Chain Home was the primary research and development focus, AI was plagued by chaos and mismanagement. The project was too secret to bring in industrial partners who might have helped, and who instead received

---

[137] *Ibid*, 190-191, 209; Zimmerman, "Information and the Air Defence Revolution," 389-391

[138] Zimmerman, *Britain's Shield*, 211-224; Dowding, "Despatch," 4560

cryptic orders (like to design alternators that looked like an aircraft DC generator).[139] When Chain Home went operational and management was turned directly over to RAF officers in 1939, Watson-Watt's team relocated from Bawdsey to Dundee, which severely disrupted AI research. The demoralized scientists got caught up in installing the inadequate Mk 3 AI which had been rushed to production, rather than researching improved AI designs. Both Tizard and Dowding understood the night-fighting limitations of their system, but without a workable AI, there was little they could do.

The Air Staff informed Dowding on 13 November 1940 that he was being sent to the United States to improve air forces liaison, effectively being relieved of Fighter Command. Controversy has surrounded the ignominious dismissal of the hero of the Battle of Britain and his key lieutenant Keith Park ever since, but it's clear that the failure to stop the Night Blitz was one of the major reasons.[140] The irony is that Dowding understood how to solve the nightfighting problem better than his detractors, but the AI research effort was too fragmented in 1940. An improved Mk 4 AI set would not be available, along with the new Bristol Beaufighter, until 1941. From 2 March to 13 April 1941, Fighter Command shot down at least 32 aircraft and damaged a dozen more; before the Mk 4, there had been only 6 kills.[141] Dowding's system proved unable to connect with the Luftwaffe at night, but there was little he could do about this unfortunate insulation. Fortunately for the British, Hitler had already given up on Sealion and turned his attention east. Britain was saved by the bell.

8.5.3 Initiative

Clearly Fighter Command was not immune from information friction. Destabilization of the information problem and dysfunction in the sociotechnical solution are inevitable once "the balloon goes up." Fighter Command's system continued to perform, nevertheless, because participants within it were continually tinkering. The connective tissue of this distributed information system was human, and Fighter Command was able to lower the barriers between technical expertise and operational demands to make new connections when possible. Watson-

---

[139] Such insular secrecy also plagued aspects of Chain Home development like station site selection, writing design specs, overseeing manufacturers, setting up electronics, and so forth, which exacerbated the calibration problems discussed above; Zimmerman, *Britain's Shield*, 126

[140] John Ray, *The Battle of Britain, New Perspectives: Behind the Scenes of the Great Air War* (London, U.K.: Arms and Armour, 1994)

[141] Zimmerman, *Britain's Shield*, 224

Watt described his philosophy of experimental research and development as "The Cult of the Imperfect," and this could apply equally well to the expedient operation of the system as a whole.[142] Fighter Command "was simultaneously undergoing construction, upgrading, expansion, experimentation, training, operational testing and operations."[143] That is, practitioners were taking the initiative to perform "runtime design."

8.5.3.1 Skilled operators

The best way to link technical expertise to operational needs is to do so in the same skull. When operators understood the technical details of the machines they were using as well as the tactical problems to which they were trying to apply them, then they were able to detect nuances and opportunities that less skilled operators would miss. Sector room controllers were themselves pilots; while this created some resentment in the Signals Branch among those who saw controlling as a radio task, the pilot-controllers were better able to understand the tactical situation of the fighters they controlled. They were thus able to deal with unforeseen situations by simulating in their minds what the pilot on the other end was doing. In order to keep its radios up and running, the RAF launched a selective draft of civilian ham radio operators, of which there were many in Britain, to be radar technicians and DF operators. Already enthusiastic about nursing fickle radio technology along in their free time, they were able to continually tweak the radar and radio sets they worked in an official capacity.

I mentioned above that filtering was a particularly complicated art, requiring a sound grasp of radar, pattern matching skills, and experience; the identity and direction of tracks depended upon filterer's intelligence and discerning judgment. The first filter operators were non-commissioned officers who happened to be very talented individuals, but this turned out not to be the norm for RAF NCOs. The quality of filterers was a serious problem until Fighter Command required that officers with higher education fulfill the job (They were ready only by June 1940, just in time!). All of these jobs involved a lot of judgment and intuition, and the operators who performed them needed to understand both the technical supply and tactical

[142] *Ibid*, 79
[143] *Ibid*, 172

demand sides of their work. Fighter Command worked to ensure that its operators were both technologically savvy and operationally focused.[144]

8.5.3.2 Expedient Solutions

Scientists and operators invented and implemented various types of new machinery and technical adaptations as problems cropped up. Usually they relied on the resources that were locally available. A lot of the radar research depended on off-the-shelf commercial components, especially from television (like CRTs). The "fruit machine" mechanical tabulator which automated the conversion of angles and ranges into height and coordinates at the radar stations emerged as a prototype only in November 1939. "Many ingenious devices, including optical converters, and calculators, too numerous to describe here, were introduced in the latter stages of the war which made the Chain Home system extremely efficient and reliable."[145]

Process innovations were common as well, such as the "X" designation for unidentified tracks to avoid the previous default to hostile. One of the most important was the invention of "macroscopic reporting" in the Filter Room to deal with the problems of large formations: rather than trying to track every single aircraft, which was becoming impossible because of saturation, the raid track would include an estimate of the number of aircraft in the formation. This change highlights the fact that the "truth" of a symbol has more to do with what sort of action it can effectively coordinate in context. "The real position" of the aircraft was collapsed into an aggregate measure that could actually be kept in rough coordination with the structure of the real-world moving raid. It would be up to the intercepting squadrons to disaggregate this quantity. Another important process innovation was the creation of a "Lost Property Office" to maintain a separate plot of tracks which had dropped off the main Ops Room plot. The main plot never displayed any information older than 15 minutes by the color-coded clock, but some raids just managed to elude detection more than once or twice. Tracks that crossed sector boundaries or that were handed off from radar to the observers, or which were only detected by observers in the first place, were particularly liable to get lost. The "Lost Property Office" plot

---

[144] Wood and Dempster, *Narrow Margin*, 75, 121; Zimmerman, *Britain's Shield*, 183; Zimmerman, "Information and the Air Defence Revolution," 387; Beyerchen, "From Radio to Radar," 285

[145] Neale, "CH," 81 (quote); Zimmerman, *Britain's Shield*, 185; Beyerchen, "From Radio to Radar," 282

was something of a mess, but it enabled some of these feral tracks to be reacquired in time to intercept them.[146]

8.5.3.3 Operational Research

Civilian scientists were involved in many of the runtime modifications cited above. Fighter Command enjoyed an unprecedented level of interaction between scientists and military personnel. Whereas science had previously been applied to crafting and testing individual weapons in military history, the Battle of Britain was the first time that science was applied systematically to force employment, previously a purely military task. The term "operational research" was coined by Watson-Watt in 1938, and succinctly defined by Dowding in November 1940: "The war will be won by science thoughtfully applied to operational requirements." There were precedents in the Lanchester equations and Admiralty efforts to optimize fleet deployments, but it was never focused and retained like it was for British air defense. OR became an important part of the entire Allied war effort.[147]

Fighter Command was simultaneously a scientific laboratory and a warfighting command. The free flow of knowledge between scientific and military cultures was established early in the 1935 move of radar research from Orfordness to Bawdsey, which meant that the center of scientific research was itself also an operational Chain Home station. Tizard was the personification of easy translation between the two cultures, with his tactical experience in the Royal Flying Corps and credentials as a scientific administrator with the government. As Chain Home management transferred to the RAF in mid-1938, the scientists spent more time on OR. They worked with the radar stations to figure out better ways to operate and calibrate the gear, with the result that the stations with a scientist in residence were always the top performers in the chain. They studied filtering processes and analyzed every raid that escaped radar detection, discovering various problems and recommending solutions to improve filtering, plotting, and telling. They established close working relationships with operators and officers and became part of the active nervous system of Fighter Command. The establishment of the "OR Section, Fighter Command" embodied the unprecedented step of military officers regularly asking for scientific advice on their operational force-employment problems. The emergence of a discourse

---

[146] Zimmerman, *Britain's Shield*, 173, 180, 201

[147] Wood and Dempster, *Narrow Margin*, 116; Kirby and Capey, "The Air Defence of Great Britain, 1920-1940: An Operational Research Perspective"

of information systems, which saw humans and machines as processing components in large-scale rational system, provided them with a common language to describe and to optimize interactions throughout the system. One OR study of Fighter Command in 1948 estimated that radar improved the probability of interception tenfold while OR contributions doubled this probability again. The radar scientists began by experimenting with a new technology in the Orfordness laboratory and ended up experimenting with a broader sociotechnical system in the middle of a war.[148]

Information friction theory expects that practitioners will act like amateur ethnographers. They should regularly switch their attention between the content and the format of information systems, paying attention now to what information means, and then to how information works. They have to attend to the details of sociotechnical architecture if they want to create knowledge that enables reliable repeated reconnection with the world. In Fighter Command, the OR scientists were conducting just this sort of pragmatic ethnography. They observed sociotechincal processes in action, described and analyzed them in detail, often relying on simple optimization models, and then recommended ways to improve processes.

For example, an important January 1940 study on Filter Room organization found that it "had gradually receded from its original function as a purely technical room" and become "more of an operations room than a filter room, and contained all sorts of people and devices [that had] nothing whatever to do with RDF." The scientists observed "appallingly low standards of filtering" that led the filter officer to constantly interfere and ask the tellers for the same information they had just provided the filterer. OR scientists did not just assume that the Filter Room was operating as expected, but they went and looked at what was actually happening. Through close observation, they helped to clarify what the operational knowledge needs actually were when the operators themselves had difficulty doing so. The report caused Fighter Command to raise standards in filterer recruitment and training, as mentioned above. OR scientists were, in essence, recommending ways to reprogram the sociotechnical machine while

[148] Wood and Dempster, *Narrow Margin*, 83; Zimmerman, *Britain's Shield*, 50-51, 159, 179; Kirby and Capey, "Air Defence of Great Britain," 562-4

it was running, and to do so they had to observe what was actually going on between humans and machines.[149]

The boundaries between IT expertise and operational knowledge needs were very low for Fighter Command's C2 because the people who were building the system were working side by side with, and sometimes were the same as, the people who were operating it. A continuous stream of bottom up process and product improvements helped to restabilize a system which was constantly subject to wartime destabilization. Expedient adaptation was an active process in Fighter Command.

8.6 An Integrated Enterprise

Fighter Command's C2 system was an impressive achievement. The official British history rightly called it "the most efficient scheme of air defence in the world at the time,"[150] and when the processing time and accuracy of the system spelled the difference between a successful interception and an unhindered raid, then efficiency was also effectiveness.[151] The RAF's adoption of new IT networks seems to have provided the sort of improved situational awareness and rapid decision-making that RMA theories predict that networks should provide. British fighters outfought the Germans because they knew more. A network of sensors and the ability to share information through standardized protocols allowed the RAF to fight with far fewer fighters than it would have otherwise required (and which were not available). The C2 system allowed Fighter Command to substitute information for mass, a statement that can perhaps be measured in the fact that the RAF won the battle on only half of the 120 squadrons that it estimated it absolutely needed before the war. Churchill's famous "few" were backed up by several tens of thousands more working to produce and disseminate knowledge of Luftwaffe raids throughout Fighter Command. This network of many knowledge workers enabled the "few" combatants to be in the right place at the right time. Of course there was still a lot of noise in the network, and many raids got through, but the RAF had a relative advantage. Dowding observed, "In spite of these handicaps, however, the system operated effectively, and it is not too

---

[149] Zimmerman, *Britain's Shield*, 182

[150] Kirby and Capey, "Air Defence of Great Britain," 564

[151] Many people make the point that militaries care more about effectiveness than efficiency: war is about winning and is often quite wasteful. There is less of a dichotomy between the effectiveness of decision and the efficiency and accuracy of decision-making in time-critical situations. When seconds matter to the battlefield result, then efficiency then enables effectiveness.

much to say that the warnings which it gave could have been obtained by no other means and constituted a vital factor in the Air Defense of Great Britain."[152]

Fighter Command's C2 system relied not just on an innovation in IT—although radar and DF were essential—but even more on innovation in organization. The British created the idea of an engineered "information system" composed of humans and machines processing symbols together, and they worked untiringly to optimize its performance for the task of air defense. The centralized C2 was indeed architected—its foundations were laid down in World War I—but it was also an organic system capable of making sense of breakdowns and learning. Humans were the connective tissue amongst the machines, and they were able to compensate for frequent problems when the implementation of design abstractions didn't quite conform to standards in practice. The system is thus a very nice example of distributed cognition: humans and machines together implemented a representational solution to the problem of computing raid interceptions. "Centers of calculation" integrated perception and articulation "cascades of inscription," and practitioners collectively adjusted to breakdowns they experienced.[153]

Information friction theory explains the success of the Dowding system. The theory argues that successful C2 performance requires three conditions to be met. Fighter Command's C2 was successful by historiographic consensus, and sure enough, we find that it met the three conditions. The theory passes this important "hoop test."

Air defense was a relatively stable problem, as evidenced by the constancy of basic concepts of operation across two decades of regular exercises. Air defense "objectively" has a simple ontology of types, properties and relationships: there are few types of things to track in the world (friendly and enemy aircraft) and only a limited number of things they can do, constrained by physical laws. As long as it was possible to connect early warning systems to incoming aircraft, then centers of calculation could build up simple representations, constrained at each transformation to preserve referential integrity to the geometry among aircraft in the sky. This internal analog of the external world enabled controllers to successfully vector fighters to an

[152] Dowding, "Despatch," 4546

[153] In tracing these interactions through a system operating in wartime, we see both the utility and the limits of the "social construction of technology" concept that figures centrally in the sociology of technology. Indeed, humans fashioned the institutions that shaped technological development, which was directed for particular purposes through the resolution of controversies. At the same time, hard constraints in the world matted and it made sense to talk about the veracity of representations were mistakes could prove lethal.

interception. Air defense is a sweet problem for IT automation. The increasing speed of bombers threatened to seriously undermine existing methods of connecting the system to targets in time for interception, but radar arrived just in time. Radar did not change the problem; it merely restabilized a problem that the RAF already understood well. The Germans were also "cooperative" in not systematically attacking the system, which would have been destabilizing indeed.

Some political controversies threatened to undermine internal consensus about how to solve the air defense problem, or whether to even solve it at all. It turns out that the RAF strategic bombing bias did not impede the systematic preparation for defense so much as has commonly been believed. RAF doctrine was not the greatest obstacle to effective air defense. The Lindemann-Tizard dispute was far more dangerous, for it could have undermined the entire radar research agenda. It was not enough to want defense, as the RAF and (even more) the civilian politicians did, for the radar instrument had to be built and debugged. Lindemann's bad scientific advice and venal jealousies of Tizard, when combined with Lindemann's political connections to Churchill, could have wrecked the whole enterprise. For if the Germans had found out early about radar, they could have devised countermeasures or attacked the system more effectively.

Lastly, Fighter Command had the ability to lower barriers between IT expertise and operational demand. The scientists who built the radar system actually worked side by side with skilled RAF operators in the midst of battle. Operational research in particular proved an able practitioner of expedient adaptation to overcome the interference problems of insufficient coordination as well as the insulation problems of too much centralization. They did so through amateur ethnographic observation of the system in action.

With these three conditions met, Fighter Command was able to reliably and repeatedly close its master control loop on the Luftwaffe. Dowding and Park preserved their precious fighters through a long battle of attrition against a formidable foe. Individual fighters were able to draw upon the knowledge constructed by the entire networked system for decisive advantage.

Before getting too excited about these positive RMA results, however, it is critical to bear in mind that the RAF still had to fight it out. The British did indeed prepare for the right war—

sometimes it's OK to prepare for the last war—but the Germans could have made it much harder on them. The Germans believed that their offense had the advantage, but it didn't; the stability of the British information problem was greatly helped by German misperception of that stability. Fighter Command C2 was not solely responsible for the British victory, either, for had the British aircraft industry not been able to churn out so many Spitfires and Hurricanes, then the fighter exchange ratio, which favored the Germans, could really have started to bite. Other oddities mattered as well, like the fact that half of German casualties after September were caused by weather and ice rather than the RAF.[154]

The RMA-like effects of Fighter Command's C2 networks tipped the scales in the RAF's favor, and did so because the system met the three conditions of information friction theory. The RAF had to endure a lot of hard fighting, nonetheless, and it could have been far worse but for some luck and considerable information friction on the German side. Therefore even the success of this story should still leave us wary of RMA claims. War is hard, even when IT makes it a little bit more manageable.

[154] Overy, *Battle of Britain*, 106, 123, 125-7

Chapter 9: Conclusion

Modern digital IT doesn't determine performance improvements but rather just makes timeless dilemmas more acute by increasing their complexity. Expectations of improved knowledge through more sophisticated IT often run afoul of complexity on the battlefield and controversy in the bureaucracy. While the fundamental tensions of IT usage cannot be avoided, there are measures that organizations can take to damp the severity of oscillations between desirable and pathological outcomes. Organizations should take measures to enhance bottom-up user innovation in information systems, and they should cultivate greater awareness of how these systems both constrain and enable their behavior.

This concluding chapter will proceed in three parts. First I compare the two empirical cases, focusing on the differences in the causes of information friction which led to outcomes opposite of those expected by simple technological determinism. Second I discuss some of the open theoretical questions left by this dissertation, which has provided concepts to explain IT and battlefield performance. Third I discuss the policy implications of these ideas, organized in terms of the causes of information friction with an eye towards lessening its intensity.

9.1 Case Comparison

The two cases in this dissertation have mostly opposite values on the causal variables—external stability, internal consensus, and expedient adaptation—and opposite battlefield performance outcomes. Technological determinism does not explain this difference, but information friction theory passes both of these tests.

9.1.1 Technological Determinism

The "Revolution in Military Affairs" (RMA) is essentially a determinist idea. Most RMA proponents are quick to insist that Joint doctrine for network centric warfare is critical for wringing the military potential from IT, and thus there is an organizational component to "transformation." They might more charitably be called technological enthusiasts rather than determinists. Nevertheless, a key underlying assumption remains that IT enables radical, discontinuous improvements in military performance; therefore, the "right" doctrine merely unlocks the inherent potential.

The two cases here show that a purely determinist view of IT—admittedly more than many RMA supporters would endorse but useful for theoretical clarity—is untenable. If IT advances alone improved military performance, then we should have seen better results in modern-day Iraq compared to 1940 Britain. In fact we have seen the opposite. Advanced networks, the latest digital IT, and an ostensibly Joint organization were not able to run the targeting cycle—the area where RMA doctrine expects to see the greatest improvements—efficiently enough to shorten the duration and lessen the cost of the war. Fighter Command, by contrast, put together a hierarchical top-down system with rudimentary radios and manual plotting systems that significantly improved the situational awareness of commanders and fighter pilots, a major contribution to the defeat of the Luftwaffe.

RMA defenders can argue that this is not a fair comparison because I have picked too hard and confused a problem in Iraq and too obvious a success story in Britain. Counterinsurgency is always messy and protracted no matter the vintage of the IT. Yet that argument merely turns our attention away from technology and toward the radically different contexts of employment. Technology alone cannot explain the disparity in performance. The radically different context does raise the serious question about what is doing the work in each case, but I have not designed this research to tease out the relative importance of contextual variables. I have designed it to show how factors at three levels of analysis—structure, bureaucracy, and human-computer interaction—can all shape the struggle to align representations of the battlefield with the battlefield itself above and beyond technical capabilities.

9.1.2 Problem Scale and Complexity

The two cases feature very different external problems. The 1940 case is both a much larger scale problem and at the same time much simpler. The British played defense at a fixed site, while German airplanes attacked mainly from across the channel. They had the luxury of fighting in a homogeneous medium that lent itself well to modeling on a centralized mapboard with abstract icons for raids; everything other than friendly and enemy aircraft and sector boundaries could be ignored as irrelevant to the battlefield problem. Because it was a large scale problem, the British could develop standard operating procedures to deal with situations that they

saw repeatedly. German raids differed only slightly in their tactical details along mostly known dimensions, and thus they presented familiar scenarios again and again.

The SOTF in Iraq by contrast dealt with a small-scale and very granular problem. Furtive underground insurgencies mingled with a local populace with capricious loyalties working through myriad corruption and tribal patronage dynamics. The SOTF played offense against targets which were difficult to find and identify, and often it was distracted by unimportant targets which were easier to locate. The battlefield was quite heterogeneous, full of many different Iraqi and coalition elements with tangled lines of influence. The complex and dynamic ontology of this system resisted stable abstract modeling. Individual raids, although affording some tactical standardization, usually involved idiosyncratic situations and thus target folders and supporting intelligence with unique features and combinations.

Were it possible to transplant the SOTF's technology to the British problem, then it would be a different case entirely. Improved IT in the British case would have enabled the operations research scientists to find ways to even further reduce the information friction they did experience as raid tracks were dropped in filtering and telling. This counterfactual highlights the interactive nature of war. Because the SOTF's perceptual acuity was perhaps better in some absolute sense because of ready ISR coverage and the ability to quickly communicate records of collection across internets, at the same time its enemy sought out dead space at a far more granular level and pressed ahead with tactical and technical adaptations. The structure of the 1940 air defense problem gave the British the luxury of dealing with a coarse and stable problem, while the 2007 SOTF had to pay attention to more and more changeable details if it wanted to catch its targets and avoid negative blowback.

9.1.3 Command Autonomy

Fighter Command largely owned the air defense problem. All of the intelligence (with the exception of SIGINT) and all of the fighter defense assets were centralized under Hugh Dowding. The interwar doctrinal debates of strategic bombing vs. air defense were settled in time for the war, so Dowding and the radar scientists were able to put together an integrated system. Integration was sometimes challenged by the sheer scale of air defense, with individual radar stations resisting standardization and uneven filterer performance, but unity of command was in fact achieved and reflected in the information architecture. This same architecture—with

many of the same commanders and operators in place—remained in the fight from its beginnings in June through its culmination in September.

The SOTF, by significant contrast, controlled only a very small part of the counterinsurgency problem, and even that required tremendous coordination with the Marine Corps battlespace owner and its own special operations chain of command. The SOTF had some organic intelligence, but the majority of its perceptive take came from other producers who weren't necessarily tailoring it for SOTF consumption. While the SOTF had a strong doctrinal preference for "kinetic" commando operations, still it had to operate with the Marines who had by 2007 quite internalized the "non-kinetic" or "population-centric" mode of counterinsurgency. SOTF attempts to enhance autonomy by pursuing its counternetwork preferences, which it could do by leveraging its secrecy and resource endowments, did not map cleanly onto the contours of the objective problem where community and insurgency structures were quite intertwined. The SOTF—and the specific SEAL squadron which ran it—were just small parts in a much larger effort. As rotation after rotation went through, a lot of corporate knowledge was lost in the turnover.

9.1.4 Technological Base

Fighter Command's IT consisted of electromechanical radar, radio, telephone, and tabulating machines, as well as paper reports and plotting boards with physical tokens. While clearly more rudimentary than the SOTF's digital internets, ISR constellations, and flexible software packages on multiple laptops on ever desk, Fighter Command ironically may have enjoyed some advantages thereby. Inputs from radar stations and observer centers funneled into a central location at Bentley Priory. The Filter Room and Ops Room map tables were consolidated sites for fusion where the state of information in memory was the display itself, and this display was large enough that many people could gather around, some in raised galleries, to appreciate the single air picture. This centralized picture was well suited to the clean defensive problem fought by a single hierarchical organization. The operations research scientists were technical experts who lived and worked among military operators, helping them to expediently adapt the information system for gains in efficiency (and in thus effectiveness in this case).

The SOTF, by contrast, had no such single site for fusion. Its information processing was far more fragmented across digital networks of different classification, across a wide variety of

applications which could represent only partial views of a problem, and across different staff members' machines working on their narrow portions of different missions. Every user at every laptop, filled with many powerful applications, could gather up cascades of inscription to fashion new representations, and so they did, but the results were usually not commensurable. Special operations culture encouraged improvisation and bottom-up initiative, but had only *ad hoc* technical expertise in the workforce because the "tech" vs. "operator" totem undervalued information work. Personnel used available IT to, inadvertently, fragment the organization's view of the battlefield. Whereas Fighter Command's technical capacity supported centripetal concentration, the SOTF's IT generated a centrifugal force which its management did not check.

9.1.5 Outcome

The outcome of the Battle of Britain is unambiguous. The British successfully defended, the RAF survived, and the Germans could never think seriously about a land invasion. The reasons for the success are many, but historians agree that the command and control system was a critical factor. Tactical British fighters knew more than their adversaries because of the network supporting them. This is a qualified RMA-like success. At the operational level, it still had characteristics of a campaign of attrition. The British fought on for months, often with much friction in the system. The Germans made many mistakes that helped the British—especially their failure to understand and attack command and control—but they were still formidable and inflicted friction and pressure on their opponent. As expected by information friction theory, the battle was thus a drawn out affair, not an RMA knockout blow. Yet the system's repeated ability to enhance the tactical situational awareness of pilots via the operational situational awareness of sector controllers, and thereby to enable tactically advantageous maneuver again and again, provided Fighter Command the wherewithal to survive the Luftwaffe onslaught. Both sides recognized the outcome of the battle.

The SOTF's performance, by contrast, was fundamentally ambiguous. At best we cannot assess its minor contributions to removing some insurgents from the streets, and at worst it might have worked at cross purposes with Marine counterinsurgency efforts. Its insulated information systems fundamentally complicated the measurement of either outcome. Insulation implies some local tactical proficiency, nonetheless. The SOTF enjoyed minor successes along the lines of RMA doctrine in its ability to enhance commando situational awareness with "pervasive

surveillance" from unmanned vehicles and "reach-back" intelligence support, and throughout the mission to keep them located and logistically well-attended. Unlike in the Fighter Command case, however, these tactical RMA successes did not sum up to a decisive operational advantage on the battlefield. Repeated successful raids do not a successful counterinsurgency make. The SOTF found itself in an attritional campaign—albeit wasting information rather than mass and men—with a drawn out duration and ambiguous outcome of uncertain legitimacy.

9.1.6 Source Bias

I employed different methodologies in each case. The SOTF was a participant-observation study that, in combination with my prior immersion in various academic literatures, motivated my construction of information friction theory. Because I lived the case for a year between training and deployment, I had direct experience of a lot of information phenomena which would otherwise have been unrecorded and might have been inaccessible to differently-trained observers. I was looking for and I found a great deal of information friction at a very granular level. The Battle of Britain case, by contrast, was an historical study based largely on secondary sources. While I did encounter tales of coordination failure, fratricide, and various information follies in historians' accounts, information friction theory would predict that a lot of the friction would go unrecorded in their primary sources. Perhaps a trained ethnographic observer on site would have seen a lot which might have tempered my sanguine judgments of the performance of the system. The operations researchers were paying attention to and describing human-IT information processes explicitly, so there was some degree of on-site observation and reporting. I acknowledge these concerns and the challenges inherent to both types of methodologies.

Nonetheless, I have been able to provide some insight into the daily conduct of modern IT-intensive war, and to compare it to information processing in a previous era. The battlefield performances of each case—one ambiguous in a complex environment, one more decisive in a simpler environment—align well with the predictions of the theory given the conditions in each case. There is no doubt that I have provided a much finer level of detail in the SOTF case, a small organization in a limited war, than the Fighter Command case, a larger organization in a larger war. Yet such detail was necessary to be able to elaborate the theory. I was then able to test it in a very different context in Fighter Command, which by virtue of its importance and the

number of people involved is quite well-documented. This usefulness across temporal era and testing methodology speaks well to the basic soundness of the theory.

9.2 Open Theoretical Questions

This project has imported the sociology of technology into security studies and constructed new theory using ethnographic methods. I have presented a lot of concepts, posited some causal connections, and I have tested for overall plausibility, but I have hardly tested everything robustly. There are still a lot of open questions for theory building and testing. I take this to be a strength of this project, as it has opened up avenues of future research in human-computer interaction and organizational performance. The introduction identified several of the areas where I make interdisciplinary contributions. This section will identify some areas I have not developed.

9.2.1 Marginal Effect on Performance

I have described information friction as an aggregate measure of the risk of political and technical breakdown in distributed cognition, and I have described a number of its manifestations in human-computer interaction and organizational control. I have provided hypotheses on how these risks, in the aggregate, make different types of outcomes—targeting precision, conflict duration, casualties, operational style, *etc.*—more or less likely. I have not constructed detailed linkages between the specific manifestations and the specific outcome hypotheses. That's a tall order, given all the tangled causal paths in any particular case. The utility of information friction theory in its present form is that it provides concepts to help explain particular cases, not least of all by directing attention to situated phenomena which otherwise remain tacitly invisible.

Because all factors which affect battlefield performance—civil military relations, weapons quality, personnel training, *etc.*—must be articulated through a command and control nervous system to have any operational influence, information friction can be a drag on the behavioral expression of all of these things. The causes of information friction spelled out here include a lot of organizational and technical factors that others have considered in discussing military effectiveness. The contribution here is a new intervening notion to translate those factors into battlefield behavior through their effect on information processing. I have not, however, much discussed the relative importance of friction with respect to various factors; that

is, whether it is possible to tease out its marginal contribution to effectiveness, or whether that question even makes any sense given the social embeddedness of IT.

9.2.2 Relative Influence of Causes

I have used a levels-of-analysis approach to organize concepts from various literatures into causal explanations for information system performance. I have not commented a great deal on their relative importance or interaction (except to point out that internal consensus amid external instability promotes insulation friction). Is battlefield structure or organizational politics more important for generating debilitating friction? For example, the physical domain of combat seems to be pretty important for explaining the ease or difficulty of achieving command of the commons. As a consequence, expedient adaptation has its limits. Amidst internal disensus and/or external instability, runtime design is no panacea and can even exacerbate friction. There will surely be no one master cause of information friction because IT is so deeply embedded in everything a military does. The challenge is learning to see and explain this pervasive technology without over-attributing causation to its technical character alone.

9.2.3 Interaction of Components

The causal variables and information friction are aggregate measures. I have discussed each of them in turn and often in combination, but I have not made a detailed analysis of their relative importance and interaction effects. Which of these internal components tend to co-vary? Which are measuring the same underlying phenomena? Which are most important? Extracting the fine grained causal linkage would again be quite a tall order because it would be so tangled in specific cases. I have spent some time pulling these theoretical mechanisms apart, but there is work left to be done in putting them back together.

9.2.4 Endogeneity

There is some serious endogeneity in the factors of information friction: causes become effects and vice versa. This is to be expected for a fundamentally intervening phenomenon like IT usage. Some people are uncomfortable with endogenous causation, but I embrace it to explain the recursive influences between technical infrastructure and human interpretation. For analytical or at least rhetorical clarity I have presented information friction first as an independent variable in Chapter 3 and then as a dependent variable in Chapter 4, but as a holistic

notion there is a lot of entanglement between the causes and effects of friction, and between its subjective and objective aspects.

Over time, I think that this endogeneity makes information friction a cause of itself. This was apparent at a very granular scale in the SOTF case where I saw personnel moving in and out of regimes of high and low friction in an attempt to stabilize their processes. We should expect to see this at a more macro level as well. An appendix on endogenous growth offers some tentative hypotheses, but the basic idea is that the measures that an organization takes to lower friction end up creating more friction, and the supply of IT then creates its own demand. Some tangible predictions of this pervasive endogeneity are that over time, command and control systems—both IT and organizations—should become more complex, differentiated, and interdependent, with an ever greater proportion of the workforce shifted into knowledge work. Information friction—the sociotechnical struggle to coordinate representations with reality—acts as a ratchet for complexity.

9.2.5 Soft Determinism

The growth of information processing complexity sketched in Chapter 2, whether explained by endogenous growth or something else, is a pronounced historical trend associated with IT adoption. Bernard Brodie observed that "*in the long run*, technology has transformed war pretty much in its own fashion."[1] While there are plenty of contingent mistakes, tussles among bureaucratic conservatives and insurgents, and temporary imbalances along the way, militaries do tend to adopt technologies that enable better control of war once problems are stabilized and well defined. Brodie describes a sort of soft technological determinism, in which contingent choice is given tremendous influence on the course of specific events but without going to the opposite extreme of political determinism.[2] The interdependent evolution of institutions and technology creates patterns of constraint and possibility which tend to further canalize developments in a certain direction.

The RMA debate has stalled out because it's clear that IT is on the battlefield to stay and that it provides distinct advantages for many proscribed problems like fire control, navigation,

---

[1]Bernard Brodie, "Technological Change, Strategic Doctrine, and Political Outcomes" in Historical Dimensions of National Security Problems, ed. K. Knorr (Lawrence, KS: Kansas University Press, 1976), 299 (emphasis in original)

[2] For a range of perspectives on technological determinism see Merritt Roe Smith and Leo Marx, eds., *Does Technology Drive History? The Dilemma of Technological Determinism* (Cambridge, MA: MIT Press, 1994)

and administrative management. It is fair to say, with all the qualifications about the importance of social context, that IT and its challenges have channeled military evolution in the direction of increasing control in time and space and increasing emphasis on knowledge work. Organizations use IT to manage complexity, and this usage has made them even more complex (which demands more IT...). As a result, military organizations have experienced a profound shift in the nature of everyday work for most personnel from physical to cognitive labor. The reason this differs so much from the normal RMA determinism is that actual performance outcomes remain indeterminate as war itself evolves to compensate the advantages of IT and information friction become internally pervasive. More fundamentally, the employment of IT to seek battlefield advantage is rooted in the military imperative to seek competitive advantage. Students of international relations differ on whether this is rooted in the insecurity of anarchic balances of power or domestic institutions and militarist ideology. If we hold that competitive imperative constant, then we can rightly say that militaries' eager embrace of IT has indeed "transformed war pretty much in its own fashion."

9.2.6 Learning Effects

In 1987 Robert Solow quipped that computers appeared everywhere except in the productivity statistics.[3] There seemed to be no straightforward correlation between IT investment and firm output, which became known as the "productivity paradox." Thomas Landauer located the problem in myopic managerial exuberance and poor technical designs which failed to comprehend user situations.[4] Others have pointed out that the paradox is spurious because measurements do not report intangible information improvements, there exist steep learning effects and lags in putting computers to work, and industry-wide redistributions of costs mean that individual firms may benefit while overall productivity does not.[5] While this debate now appears to have been resolved in favor of enhanced productivity, it has usefully underlined that IT does not improve economic production all by itself. Erik Brynjolfsson argues

---

[3] Paul Attewell, "Information Technology and the Productivity Paradox," in *Organizational Linkages: Understanding the Productivity Paradox*, ed. D. Harris (Washington, DC: National Academy Press, 1994): 13-53.

[4] Thomas K. Landauer, *The Trouble With Computers: Usefulness, Usability, and Productivity* (Cambridge, MA: MIT Press, 1996)

[5] Erik Brynjolfsson, "The Productivity Paradox of Information Technology," *Communications of the ACM* vol. 36, no. 12 (1993): 66 – 77; Paul A. David, "The Dynamo and the Computer: An Historical Perspective on the Modern Productivity Paradox," *American Economic Review* vol. 80, no. 2 (1990): 355-361

that complementary organizational adaptations have been needed to exploit and shape it.[6] Even when IT applications enable some substitution for human intellectual labor, this is usually accompanied by the accumulation of additional complementary scaffolding to support it.

To what extent is there a lag to discover and implement these institutional complements to IT in military organizations? Some units do indeed figure out more effective ways to use their IT than others; I would expect to find internal consensus and expedient adaptive capacity in those cases, probably applied to a proscribed problem that has been externally stabilized. At the same time, changes in information friction will be changes in degree, not in kind. It can be abated or exacerbated in particular situations and for particular applications as people work to stabilize their routines and tactics. But it has a tendency to continually crop up in new ways, and for a growing proportion of the force. Information friction doesn't goes away as an organization gains experience with IT, but members may find ways to live with it and find those islands of representational stability where IT can contribute to productive output. There is much more room for the investigation of how organizations learn to deal with friction over time.

9.2.7 External Validity

I have constructed information friction theory as a general explanation for command and control performance in any military organization in any war. I have performed one detailed external validity check on the theory, but clearly there are lots more combinations of the causal variables that could be tested. In particular it would be interesting to hold the IT constant and look at differential performance of units in the same war, different cultural appropriations of IT, *etc*. The SOTF case in particular is begging for further comparison with other SOF rotations in the same province or other units more proficient at counternetwork operations in Iraq and Afghanistan, in order to make a fair assessment of that network-intensive campaign concept. I furthermore expect the theoretical concepts to get some traction in non-military cases of IT usage.

---

[6] Erik Brynjolfsson and Lorin M. Hitt, "Beyond Computation: Information Technology, Organizational Transformation and Business Performance," *Journal of Economic Perspectives* vol. 14, no. 4 (2000): 23-48; Dale W. Jorgenson, Kevin J. Stiroh, Robert J. Gordon and Daniel E. Sichel, "Raising the Speed Limit: U.S. Economic Growth in the Information Age," Brookings Papers on Economic Activity vol. 2000, no. 1 (2000): 125-235; Bill Lehr and Frank Lichtenberg, "Information Technology and Its Impact on Productivity: Firm-Level Evidence From Government and Private Data Sources, 1977-1993," *Canadian Journal of Economics* vol. 32, no. 2 (1999): 335-362

Firms and bureaucracies anywhere have to deal with information friction, even though their "battlefields" are quite different. Information friction encompasses all of the factors which cause real information systems to diverge from managerial ideals. The concepts here can help to explain the difficulty companies, their employees and customers have in adopting and standardizing information protocols as the business environment changes and as actors obfuscate their situation to others in order to improve rhetorical and competitive positions. They might also help to explain some of the more systemic risks built into our economies as we become more dependent on indirect representation and complex algorithms which elude clear and rational characterization. The underlying political economy concepts in Chapter 4 should be sharpened in order to make an argument for information friction as a generalized phenomenon.

9.3 Policy Implications

The remainder of this chapter will sketch the policy implications of this project. Information friction is an intervening factor in any sort of battlefield performance, which is what defense policymakers and military practitioners would ultimately like to be able to influence. Specific recommendations to lower information friction and thus improve performance—or at least avoid poor performance—follow from its three sets of causes described in Chapter 4: cultivate some humility in complex situations, beware of bureaucratic transaction costs, and promote mindful user innovation. All of these recommendations are starting points for further study and reflection, not necessarily airtight logical consequences of the theory, which after all stresses the importance of contingency and emergent circumstances.

9.3.1 Offensive Restraint

High information friction lowers the reliability of digital representations of the world because of IT breakdowns and politicization throughout the enterprise. Breakdowns are more likely in complex environments or dirty battlefields. It is important to not assume that IT will operate as reliably in them as in cleaner domains where the U.S. enjoys "command of the commons." On cluttered battlefields, with large numbers of entities and types of entities, with actors having capricious loyalties, and with enemies determined to frustrate friendly technological advantages, then we should expect that conflicts will be dragged out longer than expected, with higher than anticipated costs in blood and treasure, only to achieve outcomes well short of decisive.

We should have a healthy dose of skepticism for the efficacy of highly-leveraged offensive operations which depend upon the ready availability of timeless and accurate information. Visions of globe spanning intelligence networks on *PowerPoint* cartoons often encourage a sense that offense is easier and battlefields cleaner than they possibly can be. An appreciation for the real risks of divergence between representation and reality should encourage humility about what can be accomplished in the face of determined and confusing resistance.

The information friction perspective supports a grand strategy of restraint (also called offshore balancing or selective engagement). The alternative of U.S. global primacy depends thoroughly on the reliability of C4ISR architectures in situations where information friction theory expects them to be unreliable. Skepticism about the reliability of representations of the battlefield and models of the adversary should temper enthusiasm for ambitious operations. This also means that long range precision conventional weapons cannot be a perfect substitute for a strategic nuclear deterrent, because the former does not in reality replace the strategic clarity of the latter.

9.3.1.1 The RMA and Irregular War

The post-9/11 wars in Central Asia follow the pattern of misperceived offense dominance. RMA visions of rapid victory turned into protracted counterinsurgencies. The first order lesson is that overeager embrace of the classic target-centric RMA on irregular battlefields can be self-defeating. Yet there is a more interesting second order development in the emergent American style of IT-intensive counterinsurgency (COIN), or what we might call RMA 2.0.

U.S. forces have put IT to work to support a new Orwellian vision of social control through biometric census initiatives, counternetwork operations, and pervasive surveillance of the population. "Protecting the population" really means controlling the indigenous masses, where every citizen might be a terrorist. The tremendous investment in population monitoring and management technology in Iraq and Afghanistan have perhaps enabled U.S. forces to avoid recourse to some of the more egregious levels of torture so prominent in earlier eras of COIN to access hard-to-get information about human networks. Irregular wars truly are information wars which need granular data about local allies and insurgents across the entire range of political and infrastructural interactions in a society. Yet surveillance networks and a robust force protection posture have often provided U.S. forces with the luxury of ignoring this detail, enabling them

instead to focus on a simpler world of critical nodes in a shadowy clandestine network or checklists in a "logistic line of operation."

This IT-intensive alternative to the original target-centric vision of RMA came about only after a long period of learning how to combine human reporting from patrols and intelligence networks with databases and reporting architectures cobbled together for the particular circumstances. The existence of a very different sort of IT-intensive military operation shows that there was nothing inherent in the nature of IT requiring transformation. RMA 1.0 "shock and awe" hardly looks like RMA 2.0 "pervasive surveillance."

What the two RMAs do have in common, however, is a hubristic overreliance on electronic representations and discounting of dangers eminating from both external political and internal bureaucratic environments. Not only might obtrusive surveillance set the COIN force at odds with its stated goals of democratization in the host society, but also the illusion of control for strategic decision-makers may make such interventions appear more feasible than they actually are. Control technology enables us to do COIN without torture and excessive bodycounts, so we should do more of it: such an argument makes for an unfortunate justification for interminable hegemonic war. The technology-substitution strategy for COIN makes irregular campaigns rather expensive, and more perniciously, gives practitioners tools to obfuscate intractable political problems with simplistic measures of progress that are easy to brief on *PowerPoint*. This peculiar fusion of RMA and COIN—the conditions for its success and its unintended costs—deserves much greater study.

9.3.1.2 Hidden Costs of Special Operations

ISR-intensive counternetwork targeting and its associated special operations infrastructure will surely be one of the American military's enduring institutional legacies from these wars. This project casts doubt on whether it is prudent to overrely on this newfound counterterrorism technology to solve what may be intractable political problems associated with U.S. occupation of foreign ground and American unwillingness or inability to manage the allies who contribute to its problems. It is certainly true that there are SOF organizations out there which will have solved the particular technical glitches I have detailed in these pages, and which will have much improved their targeting error rates. Nevertheless, the systemic nature of the

insular target fixation I have documented in this one case can be expected to be reproduced under conditions of even greater secrecy, autonomy, resourcing, and prestige.

SOF organizations inhibit the evaluation of their targeting methodology and their performance in the broader institutional context of civil war, first by inhibiting auditing through excessive secrecy and second by insulating themselves from meaningful feedback which doesn't accord with their doctrinal preferences for commando glory. Counternetwork targeting cycles can be iterated *ad infinitim* with endless tactical successes—as suggested by the steady stream of high value targeting in Iraq and Afghanistan reported in the press—yet they make what can only be seen as an ambiguous contribution in the course of these endemically protracted wars (otherwise conditions would change after important insurgents were rolled up, or cumulatively).

With such eager, well-funded, and seductively secret forces, there is serious risk that policymakers will be tempted to reach for SOF panaceas without properly evaluating their counterproductive consequences. There certainly are situations where this potent capability could and should be employed—perhaps when the clandestine network in question is not so thoroughly interpenetrated in a resentful local population, or when the strategic goal is simply to bag a particular target like Pablo Escobar or Manuel Noriega—but at present the dangers of situation-capability mismatch are woefully underappreciated. More study of modern SOF in its organizational, cultural, and operational context is urgently needed. Unfortunately, the data needed to analyze the effectiveness of coutnernetwork operations and to describe the proper conditions for SOF employment is quite simply not openly available.

9.3.1.3 The Rise of "Informatized" China

Network-centric warfare is tailor made for Pentagon scenarios of conflict with China. This is not all that surprising given the Cold War roots of RMA doctrine: the Chinese panda makes for a convenient reincarnation of the Soviet bear to justify continued investment in high-tech Air Force and Navy platforms that have little use in irregular war. Two of the most outspoken champions of the RMA have been Navy admirals, Arthur Cebrowski and William Owens, and the scenarios in the Taiwan Straits or Spratly Islands both involve high-stakes naval battles. The "defense of Taiwan" is defensive in name only, as the U.S. obviously has to deploy across the ocean on the offense. Doing so is good for justifying larger budget shares, but also makes for complicated operations prone to unexpected breakdowns and adversary countermoves.

The RMA vision has a strong offensive bias, but the Battle of Britain case suggests that defense might be the stronger form of war for IT networks. While China is usually painted as the aggressor in "access denial" scenarios, geography alone puts China on the defense to counter U.S. power projection. Might the People's Liberation Army (PLA) actually have some advantages in the Pentagon's preferred scenarios? The net-centric scenarios that play to U.S. strengths are not likely to be ones the Chinese would readily offer, and furthermore, offensive strikes on mainland Chinese command and control, in line with the target-systems worldview of the RMA, have all sorts of escalatory potential. Network-centric war with China would almost surely end up being far more unpredictable, costly, and drawn out than expected in warplans and perceived in electronic command and control displays. The U.S. military is utterly dependent on sophisticated C4ISR in any China scenario, and its offensive posture heightens the already existing risk of IT breakdown and politicization.

There are also some interesting questions of what the Chinese appropriation of RMA doctrine—sometimes translated as "war under conditions of informatization"—will look like.[7] When the RMA works for the U.S., it's not always for reasons put forward in RMA doctrine. Will the PLA realize that expedient adaptation is what makes the RMA work, even though it doesn't show up in the U.S. doctrine they have been busy copying and republishing? Net assessment of C4ISR is complicated in any case, but especially when assessments of PLA capabilities are stuck in an RMA doctrinal echo chamber. The PLA is sure to experience a great deal of its own information friction in any conflict scenario, and may not have the organizational capacity to work through it, especially with so little practical experience in IT-intensive warfare.[8] What, furthermore, are the interactive consequences of information friction between two extremely IT-dependent adversaries?

These scenarios are well beyond my scope to access here, but these considerations should at least encourage some humility in considering them. Humility is the antidote to hubris, and useful for abating spirals of mutually destructive mistrust and escalation.

---

[7] Jacqueline Newmyer, "The Revolution in Military Affairs With Chinese Characteristics," *Journal of Strategic Studies* vol. 33, no. 4 (2010): 483 – 504

[8] James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organiations, and Capability," in *Beyond the Strait: PLA Missions Other Than Taiwan*, ed. by Roy Kamphausen, David Lai and Andrew Scobell (U.S. Army War College Strategic Studies Institute, 2009): 253-286, notes that China's own vulnerability to information warfare is a "glaring omission" in its doctrine of "Integrated Network Centric Warfare."

9.3.1.4 Cyberthreat Inflation

The messy social scaffolding of IT systems described throughout this project renders absolute knowledge of the world unobtainable for the offense, and by the same token, it provides a buffer for the defense. Fears about cybersecurity as the Achilles heel of networked militaries overstate the potential for cyber-catastrophe as much as net-centric warfare overstates the potential for rapid victory.

Cyberdefense on a societal scale should be expected to be more robust and adaptable than rarified representations of cyberwar assume. Societies subjected to cyber-attack—which could reasonably be described as "non-lethal strategic bombing"[9]—might end up just more irritated than paralyzed. Computer users experience frustration with everyday computer glitches and compensate for them even when their systems *aren't* under serious attack, to say nothing of society's ability to compensate for electrical brownouts and financial crashes of its own devise. The original air power theory of victory through strategic bombing alone has proven historically suspect because targets often find surprising ways to compensate for the effects of bombing. Airpower is more effectively employed as a complement to other combat arms, and likewise, IT is more of a complement than a substitute for existing modes of war. Thus one wonders how the defects of pure strategic bombing theory might be repaired simply through the use of indirect, non-lethal means.[10]

Sudden paralysis of military or societal infrastructure—through the collapse of financial systems, power grids, air traffic control, military early warning, *etc.*—is unlikely, although the frightening scenario is useful in fights for bureaucratic resources and new government agencies and authorities. Cybersecurity is not the next weapon of mass destruction, and we should beware

---

[9] Thanks to Owen Cote, Jr. for this turn of phrase.

[10] In fairness to the cybersecurity literature, Espionage against military secrets and corporate intellectual property is also characterized as a dire threat, threatening "death by a thousand cuts" as adversaries copy and counter American advantages or insert malicious code into the globalized IT supply chain. This simply leads to the question of how and when espionage matters strategically, and this is not well understood, seeing as how intelligence is only one input among many to the policy process. A third theory of cyber victory is the control of ideas through marketing, persuasion, deception, or the actions of the cyber-empowered crowd (e.g., the 2007 Russian attacks on Estonia or the 2009 Twitter buzz over Iranian elections are often cited). We should then ask how and when soft power influences the hard power position of states, and the latter traditionally dominates international security calculations. All three of these theories of cyber-victory have in common some sort of indirect action through IT to cause strategic effects (*i.e.*, cyberspace→infrastructure-attack/espionage/persuasion→security); in all three the second step—regardless of the sometimes dubious technical possibility of the first—is usually poorly understood or contested in international relations scholarship.

the rampant threat inflation which accompanies the discourse. Computer security is critically important for personal privacy and the prevention of cybercrime and cyberespionage, but computer security ought not be so readily conflated with international security just because they use the same language of attack and defense.

I would offer a tentative hypothesis that the strategic complexity and ambiguity of cybersecurity actually undermines its impact on international security. Cyberspace is difficult to weaponize for targeted coercion because it is so ubiquitous and socially embedded. Contrast the unambiguous threat of nuclear Armageddon and thus the utility of nuclear weapons for strategic deterrence and bargaining.[11] Ironically, we shall likely see more cyber-shennanigans among states and others precisely because it matters less for strategic coercion, much as great powers often engage in mutually-irritating proxy wars when direct confrontation is too costly as in the Cold War.

The cybersecurity topic is far too large and technical to do justice to this argument here. This project is scoped to the preliminary task of clarifying the social context of everyday IT usage in military organizations. Both net-centric and cybersecurity versions of the RMA tend to ignore "the social life of information."[12] In war that life is especially full of friction, which makes the RMA less potent for the offense and cyberwar less scary for the defense. Nevertheless, the esoteric complexity of cybersecurity makes it fertile ground for fear mongering and lucrative bureaucratic rent-seeking.

9.3.2 The Pacemaker of Bureaucratization

The RMA looks to IT to enhance collaboration and speed decision cycles, but the "modern means of communication," as Max Weber put it long ago, are also "pacemakers of bureaucratization."[13] IT has grown up in government and corporate bureaucracy because it promises greater administrative control. Yet the process of implementation across a distributed community of heterogeneous actors often leads to greater administrative controversy and bureaucratic metastasis.

---

[11] Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca, NY: Cornell University Press, 1989)

[12] John Seely-Brown and Paul Duguid, *The Social Life of Information* (Cambridge, MA: Harvard Business School Press, 2000)

[13] Max Weber, *Essays in Sociology* (New York, NY: Oxford University Press, 1946), 213

RMA doctrine has long insisted that organizational design and operational concepts are as important as technology for unlocking the potential of networks. Technocrats schizophrenically advocate a sort of centralized decentralization, where common Joint management of system procurement and operational integration enables spontaneous collaboration among flattened organizations of "self-synchronizing" components. While this might make some sense as an abstract ideal of just enough regulation to empower efficient markets, in practice the pursuit of the former in a hierarchical but bewilderingly complex organization introduces a heavy weight of transaction and agency costs that impede the latter.

This project argues that the distinction between peacetime design and wartime usage of sociotechnical information systems is problematic, and thus so is the RMA emphasis on peacetime centralization of IT architectures for wartime decentralized operation. Innovative adaptations of doctrine and architecture must continue into wartime, and this can be impeded by the weight of bureaucratic overhead intended to preclude resort to just that sort of *ad hoc* expediency. Technically this translates into expensive but dysfunctional systems which personnel ignore, work around, or exploit only a small part of the designed functionality. Organizationally this translates into micromanagement from insulated centers of calculation with too-clean pictures of what combatants and bystanders are actually doing on the battlefield.

9.3.2.1 Enterprise Solutions are Part of the Problem

The RMA wants to have the strengths of both decentralized markets for knowledge and centralized controls on markets, but actual command and control implementations have tended to be more preoccupied with market failure than regulatory failure, with controlling security and interoperability externalities rather than bureaucratic sclerosis. As missions grow more complex and as emerging technology empowers small-scale actors both inside and outside of military organizations to manage data in surprising ways, the challenges of coordination and consensus become acute. From interservice coordination to emerging calls for greater interagency and coalition cooperation, the bar for sophisticated integration keeps getting moved up to ever more complex and politically intractable levels. The sanguine RMA condition of thoroughgoing coordination of technical protocols is never achieved, but its champions rarely look into the costs of continually piling on bureaucracy in the attempt.

Calls for system integration of enterprise architectures have been staples of command and control discussions for decades. This has ranged from the idea of a vertically integrated system along the lines of the Semi Automatic Ground Environment (SAGE) or World Wide Military Command and Control System (WWMCCS) to insistence on compliance with Department of Defense Intelligence Information System (DODIIS) standards and various modular architecture schemes. The problem with enterprise integration as an engineering design goal is it simply points out rather than solves the political problem of agreement on common standards. It's one thing to say that all stakeholders should embrace the public goods of compatible, reliable, secure information-processing, but it's quite another to actually get actors to agree to contribute to that goal when they are constantly tempted to defect to pursue private gains with their own protocols. Commercial IT and discretionary resources for information-processing throughout the labyrinth of organizational subunits in the DOD makes defection easy. Sometimes that defection is even adaptive on the battlefield as user innovation.

Any system architect would like to have: agreement on the objectives of command and control systems; few actors involved in crucial architectural discussions to ease negotiation; unity of command over critical design choices and operational art; well-defined "lanes in the road" with commensurable, comprehensive, formally-defined data definitions; rationally managed economies of scale; and secure, auditable systems. Yet the ambitious pursuit of these goods founders upon: incompatible understandings or definitions of goals; many and fluctuating numbers of interdependent stakeholders not cleanly integrated into a single chain of command; fragmented and idiosyncratic data schemes dependent on tacit knowledge; costly rent-seeking among defense contractors, legislators, and officers with parochial service or branch interests; and a heavy dead hand on the keyboards of administrative systems.

The technocratic pursuit of enterprise integration has a built-in bias for trying to get complex information architectures right at design time, which is impossible, rather than designing them for runtime adaptation, which is going to happen anyway, especially as missions and IT grow more complex. As militaries reach for digital means to automate more and more of the standard operating procedures which are their lifeblood, leaders must beware of the creeping empowerment of administrative process over operational substance. Bureaucratic sclerosis perversely acts as a negative filter on talent, furthermore; creative agile minds become frustrated

and leave early, while those who can tolerate inefficiency are promoted, becoming more invested in perpetuating the system.

9.3.2.2 Enabling Technology also Contstrains

IT is an epistemic prosthetic. It enables people and organizations to perceive entities and trends at scales of space and time that wouldn't be otherwise available. But in the process and over time, complex information architectures also build in assumptions about how the world shows up and how personnel will behave with IT and one another. Constraints, in general, make it possible to perceive the world by bringing it into focus. By the same token, they must also leave other parts of the world out of focus. Organizations build up their constraining structure not only in the software which encodes the machines' contribution to collective behavior, but even more importantly in the regular reenactment of representational genres and forms which reinforce how and when data is massaged into knowledge.

The centrality of the *PowerPoint* brief is perhaps one of the most obvious examples in modern military life. Often disparaged, the application is deeply embedded not only as a presentation tool, but also, as I explained in Chapter 6, as an ersatz database for regularly repeated missions, patrols, and targets, and as a venue for staff coordination and information updating. Yet the question must be asked: if the cultural practice of giving and taking briefs were not so central in staff life, would there be the same eagerness to exapt *PowerPoint* to store templated data? Hardly anyone would say that they enjoy "death by *PowerPoint*," and yet there is remarkably little awareness or attention given to the ways in which the application is embedded in the broader social and cultural world of the military, and which thereby make briefing sessions so central to the organization. The American military has constructed for itself a culture in which it cannot do without *PowerPoint*, for reasons that have little to do with the application itself, no matter how much it might enable any given performance.

Going without IT or refraining from action are not real options. But practitioners should appreciate that the graphs, figures, and displays upon which they depend are complex sociotechnical constructions. Representational methods and protocols are vulnerable to all sorts of breakdowns, both material and political. More reflective awareness of technological constraints that enable behavior (which can then restructure constraints) can make it possible to (1) perceive ways in which those channels can also be reconstructed and reshaped for more

productive modes of sociotechnical interaction, and (2) stay alert for the suble signs of breakdown. The greatest danger is mindless persistence in the reproduction of counterproductive patterns of behavior.

This is finally a matter for leadership at all levels. Representational practice in the military has emerged somewhat spontaneously, with personnel feeling their way through while adapting the sociotechnical resources they find. Practices and norms for sending email (perhaps substituting passive-aggressive missives for face-to-face counseling), for building briefs, and for disparaging IT savvy are self-reinforcing. As the entire organization becomes more and more knowledge-intensive, with more people in information-processing jobs rather than physical combat, it becomes imperative that leaders at all levels think a little more deliberately about their representational practices. This means not only the technical version of IT and network access policy to adopt, but the actual social processes through which data is acquired, stored, and communicated. The unguided drift of military information processing in the direction of amateurism and mutual interference is a matter of great concern. Leadership in knowledge management should the responsibility of officers at every echelon, yet too often that leaderhip is absent, and so unhealthy information habits become ingrained.

9.3.3 Forward Adaptation

The previous two categories of recommendations were mostly negative: beware the dangers of misplaced confidence in the offense and beware the accumulation of dysfunctional bureaucracy. What can be positively done to reduce information friction? Militaries should pay more attention to the third cause of information friction: expedient adaptation. Battlefields can be expected to be increasingly unstable and internal consensus can be expected to be increasingly difficult to achieve. Expedient adaptation happens spontaneously already in the U.S. military, but it should be more empowered, focused, and encouraged. We have seen many examples in these pages where unconstrained adaptation created negative externalities, so the goal of the following recommendations is to encourage a more mindful adaptation which creates positive ones instead. Again, such mindfulness ultimately requires education and leadership to inculcate into the operational force.

Technocratic systems integrators worry a great deal about controlling the negative externalities of expedient adaptation such as security vulnerabilities, non-scalable designs, and

amateurism, but not enough about promoting its positive aspects. Rather than hoping that the next "spiral release," the next "modular architecture," or the next technology champion will somehow overcome the persistent friction in operational information infrastructures, military technology communities should instead work to overcome the barriers between use and design. There is no clean line between the use and design of information systems. There are many layers and opportunities for customization. Writing macros is a form of programming. Creating *PowerPoint* templates for targets and operations is a form of knowledge-engineering. User innovation has been happening for a long time in the U.S. military and will only intensify, but it has always been an *ad hoc* process with tremendous resistance from the acquisition and network management communities.

Reforms in personnel recruitment and retention as well as in technology procurement and management should promote a mindful competence among, and institutional encouragement of, the user community to guide its natural adaptive ferment in a productive direction. Low barriers to technical expertise in forward locations, open technology, and institutional support for user innovation improve the odds that bottom-up adjustments will lower information friction. Such measures assume that systems will break down and that they will not be well-suited for whatever specific contingency emerges at the moment it flares up, in part because that's precisely where an intelligent adversary would choose to contest U.S. strengths. Therefore, ongoing information harvesting and adjustments should be required: expect to fail and plan to adapt.[14] This is essentially Clausewitz's guidance about warplans applied to their newly technical component as militaries build their assumptions about the world into IT.

9.3.3.1 Lower Boundaries to Expertise

The basic problem to address is the barrier between technical supply-side information and operational demand-side information. Just as militaries deploy with combat engineers (or Seabees) to build physical infrastructure, they ought to have organic IT engineers who can do expeditionary programming, not just mundane system administration on finished systems. Engineers up forward can see problems that aren't articulated in formal requirements, and they can prototype solutions to operationally-emergent problems. They would be not just observers,

[14] Lawrence E. Mccray, Kenneth A. Oye and Arthur C. Petersen, "Planned Adaptation in Risk Regulation: An Initial Survey of US Environmental, Health, and Safety Regulation," *Technological Forecasting and Social Change* vol. 77, no. 6 (2010): 951-959

but part of the operational staff. These expeditionary information architects—whether civilian or uniformed—would reinforce the work of engineers with program offices in the rear, contributing to the provision of increasingly-mature foundations for further innovation. Their job description would actually be much broader than just software engineering, for they would be consultants in knowledge management, which has both technical and organizational components.

The engineering aspect is, nonetheless, critical and presently quite dysfunctionally partitioned between program office design and operational use, mediated only by formal requirements. IT engineering should not only happen in a workshop separated from operations by layers of red tape. The software developer coding C4ISR systems *right now* should be on tap for users. Forward users should be able to reach back to find reliable expertise on their emergent technical design questions. Likewise, programmers in the rear should be able to reach forward. IT support budgets should include ongoing engineering support not limited to just safety or supportability concerns, but also directed toward the collaborative engineering of novel prototypes. The forward engineering concept should furthermore include ethnographers who can see and articulate how technology is used in context. This would help the program offices in the rear as well as officers in the front to better understand the real contexts of use and understand how expedient adaptation really works for better or worse in particular circumstances.

It's important to have not only technical expertise forward, but also attention to the social interactions with that technology. I have described how attention both to what information means and how it works is crucial for knowledge work as well as ethnography of knowledge work. Trained ethnographers—to include designers steeped in human-computer interaction methodologies—would be able to help engineers and managers understand how people and machines interact to realize organizational behaviors.

9.3.3.2 Intellectual Capacity

A key to controlling the negative externalities of expedient adaptation is enhancement of the intellectual capital of the force. Personnel need to be able to understand both what information means and how it works, and thus have the competence to prototype designs without inflicting problems on others. This means doing the quality-control on the front end, in the selection and training of excellent people, rather than in the back end, in the bureaucratic control of process. One difference between SOF and General Infantry is the early investment and

greater autonomy of the former to promote unconventional solutions that are nevertheless coordinated with the overall mission; control of the latter emphasizes greater rules and monitoring mechanisms to guide the mass in real time. The problems I have detailed in the SOF community come from its devaluing of information work, but its general focus on developing and nurturing talent is a useful model; the question simply turns on what sort of talent. If personnel knew how to use their IT as well as SEALs knew how to use their firepower then military knowledge management would be a different ballgame. Many personnel now use IT like novice soldiers with no muzzle discipline, threatening their comrades as they fire in every direction.

The U.S. services are in the process of developing so-called information professionals—the Navy calls its recent merger of network administration, intelligence, space systems, and electronic warfare the "Information Dominance Corps"—but these communities are composed largely of support personnel with traditionally lower prestige and training than warfare operators, and they are not selective enough. The highly process-oriented nature of military systems management, moreover, selects against creatively disruptive innovation and dilutes critical standards for knowledge evaluation. The organization actually risks repelling exactly the people it most needs: smart, inter-disciplinary, tech-savvy, operationally-minded, creative individuals interested in serving in high-impact forward operating locations.

Such a cadre could perhaps be developed the same way as special operators, but with a focus on knowledge creation and management. Selection must be highly competitive, drawing either from direct ascension programs or the warfare communities (which has the advantage of ensuring operational savvy; they might then go back to support their previous communities). Training opportunities in elite universities should be provided in the fields of library and information science, cognitive science, and political science. Graduates would be granted higher responsibility and discretion to create local knowledge management solutions while actively remaining in dialogue with engineering support in the rear. Their expedient solutions would be grounded in a solid understanding of the technology and social dynamics of information in an operational environment. These are not SEALs who also have intelligence and IT specialties; SEALs remain SEALs with commando work to do (break glass in time of war, *caveat emptor*). The idea here is to export the SEAL philosophy of excellence in training, run-to-the-sound-of-

the-guns initiative, *esprit de corps*, and a never-give-up mission focus to the realm of intelligence and command and control. A small number of talented people with domain knowledge and technical savvy would outperform scads of analysts and engineers every time (competitive analysis contests could test this proposition). To truly have capable knowledge professionals, military organizations must design the incentives to attract, motivate, exploit, reward, and retain them. The intellectual and technical problems of war are the most challenging in the world, but if a military can't attract the people to match, then it has only itself to blame for the results.

Given the trends highlighted herein of increasing complexity of missions and interdependence among esoteric skillsets, future operations will require specialized expertise that will be hard to develop in active-duty career pipelines. Official training pipelines distinguished by standardized training and vertical promotion are probably too slow to react to shifting operational timelines. The reserves are a potential source for the rapid injection of civilian expertise into operations, but they are currently structured to provide substitutes for active duty personnel rather than specialized complements. That is, reserves are currently interchangeable parts of inferior quality rather than niche experts of superior quality. The reserve system would have to be overhauled to provide a deployable pool of high-quality consultants rather than just a stock of temporary workers. Reserves presently have a well-deserved reputation among active duty for being of unreliable and unpredictable quality. Although one can cherry-pick stories about an amazing reservist who put unique civilian skills to work on deployment and made a difference, the institution is hardly set up to ensure that experience. An enlisted E-5 might be a vice president of a major multi-national corporation. An O-5 officer might be the head janitor for an elementary school. Yet they are legible to the Navy only as an E-5 and O-5 of a certain rate and designator and thus detailed to mobilization billets accordingly. Active duty personnel generally have little incentive to invest in training an individual to do much more than the minimum (stand a watch, relieve some administrative burden, *etc.*) because they might not ever see them again. It's high time for the Department of Defense to think seriously about how to improve the rate of value-added expertise augmentation, rather than relying on some genius to parachute in by lucky accident. Such a change would be bureaucratically disruptive, and is thus highly unlikely, for it would entail thinning out the existing reserve force, raising standards, dedicating more full time support to their training and administration, and refining the active-duty demand signals.

9.3.3.3 Technical Capacity

Most of the measures to improve expedient adaption capacity mentioned so far involve organizational design and personnel policy, but there are also some specifically technical measures which could help. C4ISR programs should move to open-source, open-architecture designs. Contractors should not own military code. In cases where they do, programs should insist on extensible architectures with flexible toolkits (APIs, SDKs, *etc.*) that allow programmers to leverage existing functionality in new ways. Toolkits for innovation or "mashup" which allow rapid prototyping and reconfiguration are critical.

With a rigid division between use and design, programming is not seen as a legitimate activity. Thus there are no software development packages on operational SIPRNET or JWICS nets. The proliferation of *Visual Basic* applications masquerading as Microsoft *Office* documents—the only thing approximating a development environment on operational networks—only reinforces the appearance of amateurism in user-innovators. Network administrators must control the impulse to over-manage system configurations. If the trained and trusted expeditionary engineers discussed above were present in forward environments, then there might be less concern about the admittedly serious risks of software development packages which can create executable and mobile code.

There needs to be a transparent network-based environment where problems can be documented, solutions can be proposed, and the results (both good & bad) of solutions can be communicated amongst the user community. This also allows formal programs to identify the "lead users" who are experiencing emergent trends and cobbling together prototypes to address them. Peer-to-peer technical support groups associated with the Apache webserver and Linux operating system provide precedents that might be imported into classified networks. Such a system would facilitate the reach-back and reach-forward processes needed, in addition to the physical circulation between work sites, to lower the barriers between supply and demand side expertise.

9.3.3.4 Institutionalize User Innovation

To sum up these positive recommendations, user innovation should be encouraged, not punished. Instead of relying on design in advance, military institutions should cultivate Clausewitzian genius—the ability to intuitively work through friction grounded in experience—

in sociotechnical information systems. They should organize to deal with IT breakdown, to seize emergent design opportunity, and to reconfigure amidst the friction of operations. Militaries should embrace run-time design, rather than hoping in vain that they'll get it right at design-time. IT acquisition is currently rooted in an industrial model based on bi-annual review of programs of record which starkly separates system design from system use. The line between design and use is already quite blurred by the powerful, layered, flexible, commercial IT available to operational users. Defense technocrats should embrace and support this trend by pushing technical expertise forward to rapidly prototype technologies on operational and even tactical timelines. This is not just a software concept. Any technology that has cheap, high-variety, reusable parts is a candidate for recombinatory innovation. Design occurs at many levels: hardware, protocol, application, data-structure, organizational policy, enterprise integration. All of these are candidates for user-innovation, with robust institutional support.

The U.S. Army, ever fond of popular business literature, describes itself as "a learning organization."[15] Yet in addition to the formal "lessons learned" process to which the "learning organization" concept seems to typically refer in Army discourse, learning must involve a lot of low-level debugging in the field. Rube-Goldbergism is pervasive in modern command and control, and rather than deride it as imperfect architecture, we should appreciate it as the invisible grease which makes the RMA work. Personnel will inevitably hack their systems in the normal course of operations, and so leaders should try to encourage hacks that are more often helpful than harmful. If you can't beat 'em, join 'em!

9.4 Integration is the Reverse Salient

Thomas Hughes describes the emergence of a recalcitrant challenge in large-scale system engineering as a "reverse salient," which can be political or technical and is usually both.[16] The integration of sociotechnical information systems is the reverse salient of military command and control. From Schlieffen's Modern Alexander to the modern RMA, military officers have looked to more powerful networks and information displays to improve command knowledge and thus battlefield performance. Yet this same technology has often given rise to breakdowns

[15] See, for example, U.S. Army Training and Doctrine Command, *TRADOC Pamphlet 525-5: Force XXI Operations*, August 1994; John Williams, "Is the U.S. Army a Learning Organization?" U.S. Army War College Strategy Research Project (6 March 2007)

[16] Thomas P. Hughes, *Networks of Power: Electrification in Western Society, 1880-1930* (Baltimore MD: Johns Hopkins Press, 1983)

and controversy which create uncertainty within the organization itself. A further irony is that IT is a truly ubiquitous and pervasive technology, employed in every functional area of every service since every other class of technology requires control, yet its very ubiquity renders it hard to understand and appreciate. The fish don't see the sea.

As complicated military missions and sophisticated information systems co-evolve, integration becomes the hardest phase of distributed cognition, the greatest employer of personnel, and a major source of information friction. Internal information friction will hinder modern militaries' ability to expand the zone of command into the contested zone as much as external enemy action against information systems. Information friction now affects an unprecedented proportion of military personnel and compels them to turn inward to deal with insulation and interference.

The "operational level of war," which translates strategic guidance into tactical effects, has become a major preoccupation in American professional military education over the last several decades. While it is often ambiguous in practice whether this term refers to particular echelons or organizations or the staff work they perform, the operational level can perhaps best be thought of as consisting of knowledge workers who, embedded in widely distributed control system, fight war indirectly through symbols on a map, items on a spreadsheet, and bullet points on a brief. The operational level of war will continue to employ ever larger numbers of people creating, manipulating, and communicating symbols within increasingly fragmented centers of calculation. There will be pressure not only for personnel to specialize in information processing tasks but also to overcome traditional distinctions such as the venerable operations-intelligence gap. Increasing reliance on automated vehicles for surveillance and strike will demand ever more human attention dedicated to the management of their data and control.

If professionals talk logistics while amateurs talk strategy, that talk will increasingly be of the logistics of information. This is important and unavoidable, yet there is also a risk that the mounting material problems of organizational knowledge will displace strategy altogether. Leaders at all levels should beware that the massive debugging challenges that continually emerge in information systems can also displace attention away from the *ends* or *effects* of military action. The pursuit of local optimization to prosecute available but unimportant targets can be easily justified when well-meaning practitioners are not obliged to think about their

relationship to both strategic direction and real circumstances on the ground. Greater attention to and guidance through the sociotechnical complexities of integration is desperately needed for the strategic challenges to come, but they will more likely be subsumed by the collective drift which has predominated so far. In the future, robots will talk tactics, nobody will talk strategy, and everyone will be operational.

Appendix A: Military Acronyms

Military organizations are notorious for their use of acronyms. There is some functionality in this habit, given the constant profusion of new organizations, equipment, and distinctions that constantly arise in military life. New situations, new processes, and new pieces of gear need new words. New innovations emerge through combinations of old things, thus new words emerge through combinations of old ones. An acronym provides a new word which enables personnel to distinguish, discuss, and diffuse a new concept, while preserving a modicum of provenance and self-definition. Thus DOMEX is a more handy way of referring to the analysis (exploitation) of documents and media found on the battlefield. As acronyms become routinized, provenance is frequently lost as speakers forget the original definitions altogether; thus SIPRNET (secure internet protocol router network) becomes the "zipernet."

As with all the information tools discussed throughout this dissertation, acronyms also serve some more performative or rhetorical functions. As in-group markers, those who know when to use and how to pronounce them properly designate themselves as in-the-know and exclude others (*i.e.*, can you use the latest terms properly, or are you just affecting an air of authority with something you've read but never spoken?). They become a separate dialect which outsiders cannot penetrate. In a special operations unit it might be perfectly normal to ask "Did you PID this POL this POD?" when you mean "have you validated this *PowerPoint* slide today?"[1] Acronyms also provide a sense of mastery over difficult concepts or euphemisms for controversial ones.[2]

The only other domain which comes close to the acronym fetish of the military is computer science. Like the military, this field is constantly fashioning new concepts out of existing ones, requiring some quick and somewhat self-defining means for picking out new concepts and coordinating behavior around it. Geeks also need to define ingroup boundaries. This makes the field of military IT a perfect storm for acronym generation.

[1] Literally, "Did you get a positive identification on this pattern of life this period of darkness?"
[2] This point is made by Carol Cohn, "Sex and Death in the Rational World of Defense Intellectuals," *Signs* vol. 12, no. 4 (1987): 687-718

I have tried to keep acronym use to a minimum in the main text, using them regularly just for often repeated terms that would be cumbersome to spell out (like SOF and SOTF) and otherwise only providing them parenthetically for cultural flavor.

ADCON	Administrative Command and Control
AOC	Air Operations Center
AQI	Al-Qaeda in Iraq
BFT	Blue Force Tracker
BUD/S	Basic Underwater Demolition/SEAL Training
C2	Command and Control
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Computers, and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
C4ISTAR	Command, Control, Communications, Computers, Intelligence, Surveillance, Targeting and Reconnaissance
CAOC	Combined Air Operations Center
CENTCOM	United States Central Command
CFT	(Naval Special Warfare Support Activity) Cross Functional Team
CIA	Central Intelligence Agency
CJSOTF	Combined Joint Special Operations Task Force (SOTF headquarters)
COIN	Counterinsurgency
COMINT	Communication Intelligence
CONOP	Concept of Operations
COP	Common Operational Picture
DA	Direct Action
DET	Detachment
DIIR	Draft Intelligence Information Report
DOD	Department of Defense
DSN	Defense Switched (Telephone) Network
DSP	Defense Support Program
IIR	Intelligence Information Report
DOCEX	Document Exploitation
EMCON	Emissions Control
ELINT	Electronic Intelligence
EOD	Explosive Ordinance Disposal
F3EA	Find, Fix, Finish, Exploit, Analyze
FID	Foreign Internal Defense
FMV	Full Motion Video
FOB	Forward Operating Base

GIS	Geospatial Information System
GPS	Global Positioning System
HQ	Headquarters
HUMINT	Human Intelligence
HVI	High Value Individual
IMINT	Imagery Intelligence
IO	Information Operations
IP	Internet Protocol
ISF	Iraqi Security Forces
ISR	Intelligence, Surveillance and Reconnaissance
IT	Information Technology
JAG	Judge Advocate General
JOC	Joint Operations Center
JSOC	Joint Special Operations Command
JWICS	Joint Worldwide Intelligence Communications System
LOGSU	(Naval Special Warfare) Logistics Support Detachment
MASINT	Measures and Signatures Intelligence
MCIA	Marine Corps Intelligence Activity
MEF	Marine Expeditionary Force
MNC-I	Multi-National Corps Iraq
MNF-I	Multi-National Force Iraq (Combined headquarters)
MNF-W	Multi-national Force West (Marine division in Anbar)
NIPRNET	Nonclassified Internet Protocol Router Network
NSW	Naval Special Warfare
NSWRON	Naval Special Warfare Squadron
ODA	Special Forces Operational Detachment "A"
ONI	Office of Naval Intelligence
OODA	Observe, Orient, Decide, Act
OPCON	Operational Command and Control
OPSEC	Operations Security
OPSUM	Operation Summary
PDF	Portable Document Format
POD	Period of Darkness (one day)
PID	Positive Identification
POL	Pattern of Life (also, Petroleum, Oil, and Lubricants)
PRT	Provincial Reconstruction Team
PSYOP	Psychological Operations
PUC	Person Under Control (detainee)
QRF	Quick Reaction Force
RDF	Regional Detention Facility

RFI	Request for Information
RIP/TOA	Relief in Place/Transfer of Authority
SATCOM	Satellite Communications
SCIF	Secure Classified Information Facility
SEAL	"SEa, Air, Land" maritime commandos
SF	Army Special Forces
SIGACT	Significant (Violence) Activity
SIGINT	Signals Intelligence
SIPRNET	Secure Internet Protocol Network
SITREP	Situation Report
SOCOM	United States Special Operations Command
SOF	Special Operations Forces
SOTF	Special Operations Task Force
SOTF-W	Special Operations Task Force West (Anbar Province)
SPECWAR	Naval Special Warfare
SR	Special Reconnaissance
SSE	Sensitive Site Exploitation
S-VOIP	Secret-level Voice over Internet Protocol
SWAT	Special Weapons and Tactics (Police)
TACLAN	Tactical Local Area Network
TACON	Tactical Command and Control
TIP	Target Intelligence Package
TIR	Tactical Interrogation Report
TIST	(Office of Naval Intelligence) Tactical Intelligence Support Team
TOC	Tactical Operations Center
TS/SCI	Top Secret Special Compartmented Information
TTP	Tactics, Techniques, Procedures
TU	Task Unit (Naval Special Warfare company equivalent)
UAV	Unmanned Aerial Vehicle
UDT	Underwater Demolition Team
US	United States
USSOF	United States Special Operations Forces
UW	Unconventional Warfare
VOIP	Voice over Internet Protocol
WARCOM	Naval Special Warfare Command
WERV	Western Euphrates River Valley
WMD	Weapons of Mass Destruction

Appendix B: A Mechanism Based Theory of Counterinsurgency

I developed the following model early in the deployment in my capacity as the SOTF Effects Officer in charge of tribal engagement, civil affairs, and information operations.[1] I needed (1) to describe how different missions reinforce one another in a counterinsurgency (COIN) environment, (2) with more causal granuality about civil war dynamics than usually found in COIN doctrine,[2] and (3) to describe how SOF emphasis differed slightly from conventional forces in COIN. My rhetorical goal was to persuade SEALs that the different indirect action missions they were being asked to perform in Anbar indeed enabled the direct action missions that it was in their cultural makeup to do (per Chapter 5). The SOTF staff wanted to encourage Task Units to invest more effort in non-lethal activities (given the bottom-up SOF culture, explicit direction would not give great results). This model helped to coordinate SOTF-W policy in Anbar in 2007-2008, so it's of historical interest, and it may also be of some value in the academic study of civil war.

Mechanisms that Trigger Insurgency

The model starts with the assumption, grounded in civil war scholarship and practitioner observations, that counterinsurgency war is highly localized, dynamic, and endogenously generated through the interaction of many different types of rational actors.[3] Civil war is a process of state-building and alliance consolidation at the local level where everyone is a potential strategic actor trading information, resources, and violence (or protection). It is conventional wisdom that COIN is about politics, but this is often misunderstood in terms of national or ethnic political competition, distorting perception of the local, endogenous, and more-or-less feudal dynamics which really matter. COIN is a war for popular support not because people need to be persuaded of the legitimacy of one cause or another, but because people are active participants in providing one side or another (or yet another) with information and material aid during an ongoing process of local power consolidation and state building. This

[1] I benefited from extensive conversation with Austin Long and Colin Jackson.
[2] U.S. Army Field Manual 3-24: *Counterinsurgency* (2006)
[3] Stathis N. Kalyvas, *The Logic of Violence in Civil War* (Cambridge University Press, 2006)

focuses attention on the behavior of the ambiguous and variable population between committed insurgents and government forces.

A theory of COIN requires more fidelity on how and why individuals change their level of support for one actor or another in order to manipulate these conditions. For this purpose, I found Roger Petersen's *Resistance and Rebellion* valuable.[4] Petersen begins by pointing out (as many observers have) that participation in a civil war falls along a broad spectrum from mobilization in government security forces to mobile guerrilla operations with many degrees of passive and active support in between, and that people often change their level of support over time. In some circles this spectrum is described in terms of loyalty, but it's critical to understand it in terms of behavior, because ultimately what people actually do, not how they feel, is what matters for the COIN effort.

Petersen partitions the population into those who are neutral (0), unorganized support for the insurgency (1), organized localized support (2), and mobile combat organizations (3), which are either for the insurgency or against it. Petersen's novel contribution is to describe specific triggering mechanisms which move individuals from one level of support to the next and sustaining mechanisms which keep them from backsliding. These mechanisms are derived from individual incentives based on the behavior of other people in society at large and in local community networks, and thus they change over time as more or fewer people are engaging in various behaviors. An important insight is that the different segments of the population respond to different kinds of incentives; therefore, the triggers that move a person from zero to one are different than those that move him from one to two or two to three.

The mechanisms that move people from zero to one are based on society-wide considerations, which include feelings of resentment created through status inversions or occupation (i.e., Sunni Baathists who ruled Iraq before the American invasion were debarred from government and subject to rule by the Shia whom they had previously dominated), the prestige of being a brave first mover, individual safety calculations based on the number of other people getting away with level-one behavior, and focal points to coordinate resistance rooted in culturally-specific symbols and narratives.

---

[4] Roger D. Petersen, *Resistance and Rebellion: Lessons From Eastern Europe* (Cambridge University Press, 2001)

The mechanisms that move people from one to two, by contrast, are based on the structure of local social networks. Without strong local networks (based in tribes, youth groups, professional or religious organizations, etc.), there will be no rebellion, no matter how angry individuals may feel. With strong networks, rebellion can be sustained even in the face of a more powerful government force. The mechanisms that move people from one to two include safety calculations based on the number of people in personal networks already engaging in level-two behavior, as well as norms of reciprocity, which may be unconditional as in helping out family, strong as in maintaining one's honor before his tribesmen, or somewhat weaker as in pressures for conformity. Because both safety and normative calculations are based on the behavior of others, entire groups can go rapidly over tipping points, or fail to organize at all.

The third set of mechanisms that Petersen describes sustain participation at level two, which include violent coercion and threats, and less-than-rational wishful thinking, sunk costs, and faith in repeated small victories.

Petersen gives less attention to level three, mobile guerrilla organization, other than suggesting that ideological commitment and small unit cohesion is important. To be more general, the theory must include formal guerrilla organizations like AQI and political party machines. Another feature of insurgency missing from Petersen's model altogether is economic motivation (apparently not a significant factor in the Lithuanian case).

Counter-triggers to Suppress Insurgency

Petersen's model (as amended to include economic and bureaucratic incentives) readily lends itself to deriving COIN responses in two steps. First, it is necessary to prevent people from shifting toward the negative end of the spectrum by inhibiting the mechanisms that trigger and sustain shifts toward insurgency. For example, to counter resentment formation, the counterinsurgent can include members of the newly disenfranchised group in local governance (such as regular tribal council meetings) and work to control targeting errors (false positives and indiscriminate violence). To alter safety calculations, population control (barriers to entry and movement, ID cards, biometric surveys) is critical, as is a robust intelligence program to improve targeting precision against level two and three insurgents. To counter normative mechanisms, local elites can be encouraged (perhaps through bribing them with contracts for civil affairs projects) to publically shame insurgents and lead their tribes to stand down insurgent activity.

To counter sustaining mechanisms, amnesty and protection programs for defectors and informants are crucial, as are truth-based information campaigns to publicize insurgent defeats and atrocities. To counter level-three insurgent organization, its bureaucratic processes and participants must be disrupted, subverted, or destroyed (This is a broader task than merely targeting leadership, discussed below, as a military bureaucracy is designed to expect and to replace fallen leaders.)

Second, it is necessary to encourage people to shift toward the positive end of the spectrum by enabling mechanisms that trigger and sustain shifts in that direction. Information campaigns should encourage resentment against insurgents for usurping power and resources and for committing indiscriminate atrocities, and should emphasize the prestige and heroism of people that stand up against the insurgents.[5] Such psychological operations (PSYOP) must be conducted with a high level of cultural fluency (and ideally conducted by indigenous groups themselves) to avoid negative cultural focal points and to exploit the positive ones.[6] Local self-defense groups can be formed by improving safety thresholds for participating, emphasizing the prestige of self-defense, and forming groups with some prior tribal or community association. Sustaining mechanisms to maintain government security force integrity include counter-intelligence activities, professionalization and disciplinary measures, as well as emphases on esprit-de-corps, patriotism, and combat successes.

The left side of Figure 10-1 lists Petersen's mechanisms that move people through different levels of participation in insurgency (to which are added economic incentives and the bureaucratic means of organized insurgencies). The right side of Figure 10-1 lists these COIN means to inhibit insurgency and trigger government support. These means are the inverse of the Petersen mechanisms on the right side.

---

[5] Following the assassination by al-Qaeda of Sheikh Sattar al-Rishawi, founder of the Anbar Awakening movement, posters and buttons celebrating the martyrdom of "The Lion of Anbar" and exhorting Anbaris to continue the fight appeared all over Ramadi.

[6] Iraqis can put up some effective if obscene propaganda that would never be approved through American PSYOP channels. Sometimes the best PSYOP program might simply be providing computers and printers for indigenous partners.

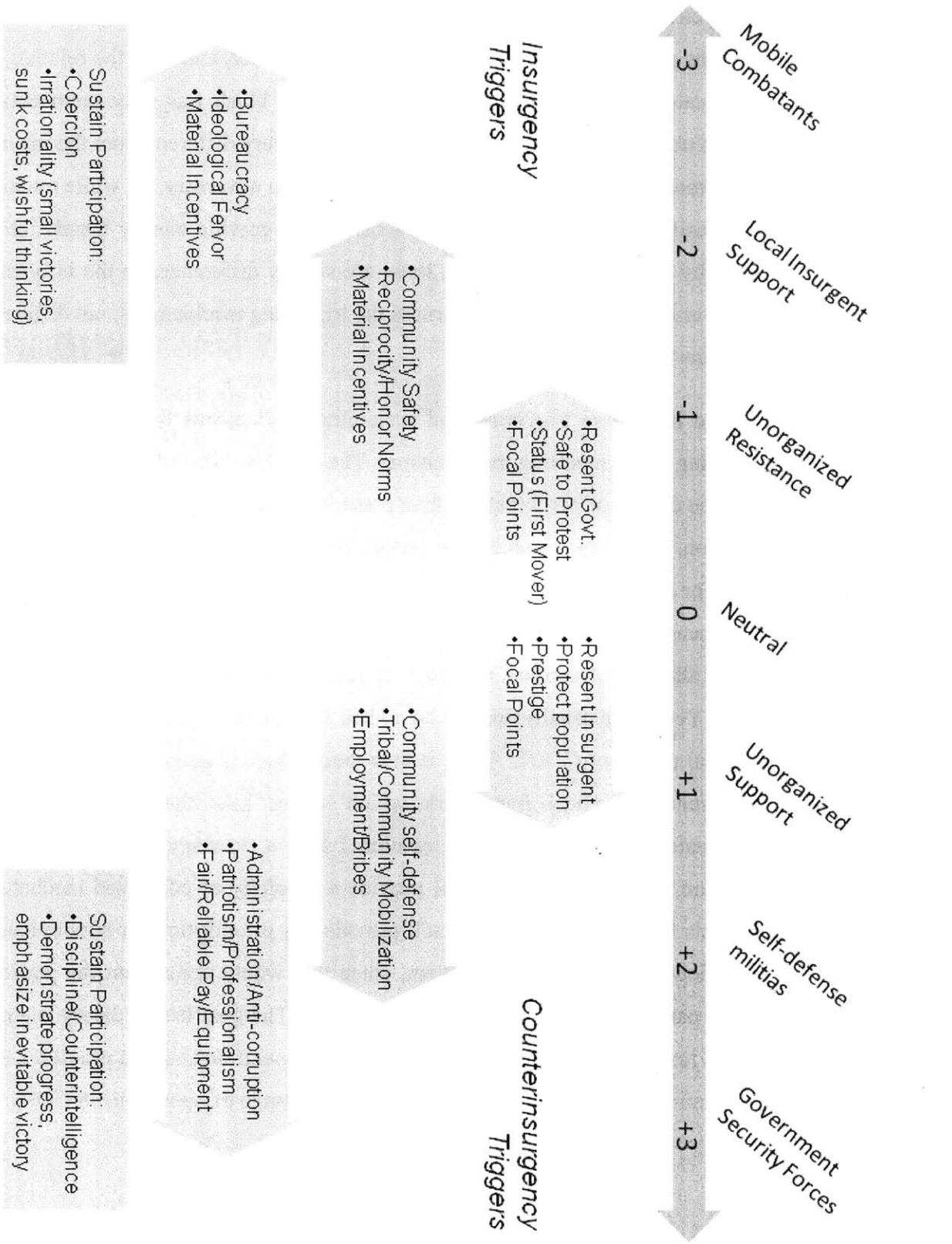


Figure 10-1: Triggering, countertriggering, and sustaining mechanisms for insurgency

A major theoretical assumption behind these pro-COIN mechanisms is that there is symmetry in the reasons people move from one magnitude to another, and only the relative level of organization and scale of the COIN actor differs. At first blush this may seem counter-intuitive, as a common observation is that the COIN problem is very different from the insurgent problem in that the former has to build capacity as well as fight an adversary, all while remaining out in the open and easily identifiable in uniform, whereas the guerilla simply blends into the population and "wins by not losing." However, these are simply differences in the information about and relative power of the adversaries to harness the triggering mechanisms, not differences in the social mechanisms themselves.

Table 10-1 also lists these triggering and sustaining mechanisms for insurgency along with the COIN inhibiting and countering mechanisms. The columns show the valence of shifts, while the rows show the degree of participation, thus preserving the symmetry between insurgent and COIN participation. We also include the organizational and economic incentives that Petersen leaves out. For simplicity, we collapse the level two and three sustaining mechanisms. None of the COIN measures listed in Table 10-1 or Figure 10-1 are in and of themselves original. They have all been described in detail in military doctrine, COIN histories, and practitioner memoirs. Yet this is usually done in an ad hoc fashion with generic comment on the complexity and political nature of COIN. What is thus unique here is gathering these measures together into a coherent theoretical framework which shows how they work within the mechanisms which create or abate insurgency: column I lists a typology of the mechanisms which generate rebellion, and columns II and III provide a typology of correlated mechanisms for its suppression. This framework cannot by itself provide any prescription for how to balance these measures and allocate resources among them, since that would depend on the particular distribution of popular participation in each particular conflict. The goal in this theory is a more preliminary theoretical justification for various types of COIN operations, and to provide a basis for the common exhortation to synergize and coordinate a wide range of operations in COIN.

Table 4-1: Insurgency triggering/sustaining mechanisms and COIN inhibiting measures

Level of Participation	I. Trigger shift toward insurgency (- ←)	II. Inhibit shift toward insurgency (→0)	III. Trigger shift toward government (→ +)
A. Unorganized support (+/- 1)	• Resentment (status inversions; indiscriminate COIN violence)	• Create political enfranchisement and honorable opportunities; Control targeting errors & protect population	• Encourage resentment against insurgents, publicize & exploit atrocities
	• Safety calculation (society-wide)	• Censure anti-government displays (can increase resentment!)	• Protect/encourage displays of support for COIN
	• Status (heroic first mover)	• Publicize insurgent atrocities, ridicule radicalism	• Emphasize COIN heroism, prestige of defying insurgents
	• Focal points (culturally-specific)	• Avoid negative focal points which resonate for insurgents	• Leverage positive focal points
B. Local Organized Support (+/- 2)	• Safety calculations (community)	• Lower safety levels for insurgents: Improve intelligence coverage, targeting precision, population control (ID cards, biometrics, barriers, etc.)	• Protect/enable self-defense groups
	• Reciprocity/honor (local norms)	• Respect legal/human rights; Engage & respect local elites, encourage elites to shame insurgents	• Encourage local elites to reinforce prestige of self-defense
	• Material incentives	• Alternative employment, bribes	• Fund self-defense groups, offer rewards for info & bounties
C. Mobile Combatant Organization (+/- 3)	• Ideological Commitment	• Reduce ideological appeal; isolate/attrite true believers	• Enhance patriotism, esprit de corps, professionalism
	• Bureaucratic organization	• Disrupt/destroy/subvert insurgent logistics, administration, and command	• Strengthen administrative capacity & reliability; fight corruption
	• Material incentives	• Disrupt insurgent finance; alternative employment	• Pay security forces fairly & reliably
D. Organized Action (Sustain at +/- 2 or 3)	• Coercion	• Amnesty programs, protect informants & defectors	• Strengthen counterintelligence and security force discipline
	• Irrationality (small victories; sunk costs; wishful thinking)	• Attrite insurgents; publicize COIN successes; discredit insurgent propaganda	• Demonstrate progress, emphasize inevitable victory

Integrating SOF Missions

The next step is to make this more practical for a SOF audience. How do the doctrinal SOF missions do the work described on the right side of Table 4-1: Insurgency triggering/sustaining mechanisms and COIN inhibiting measures? And how do these SOF missions differ from the conventional force COIN operations? Figure 4-2 shows a slide (reconstructed from memory) that I put together early in the deployment to illustrate to the SOTF staff and visitors how the different SOF missions addressed different segments of the population, as well as how SOF and conventional emphasis differed.

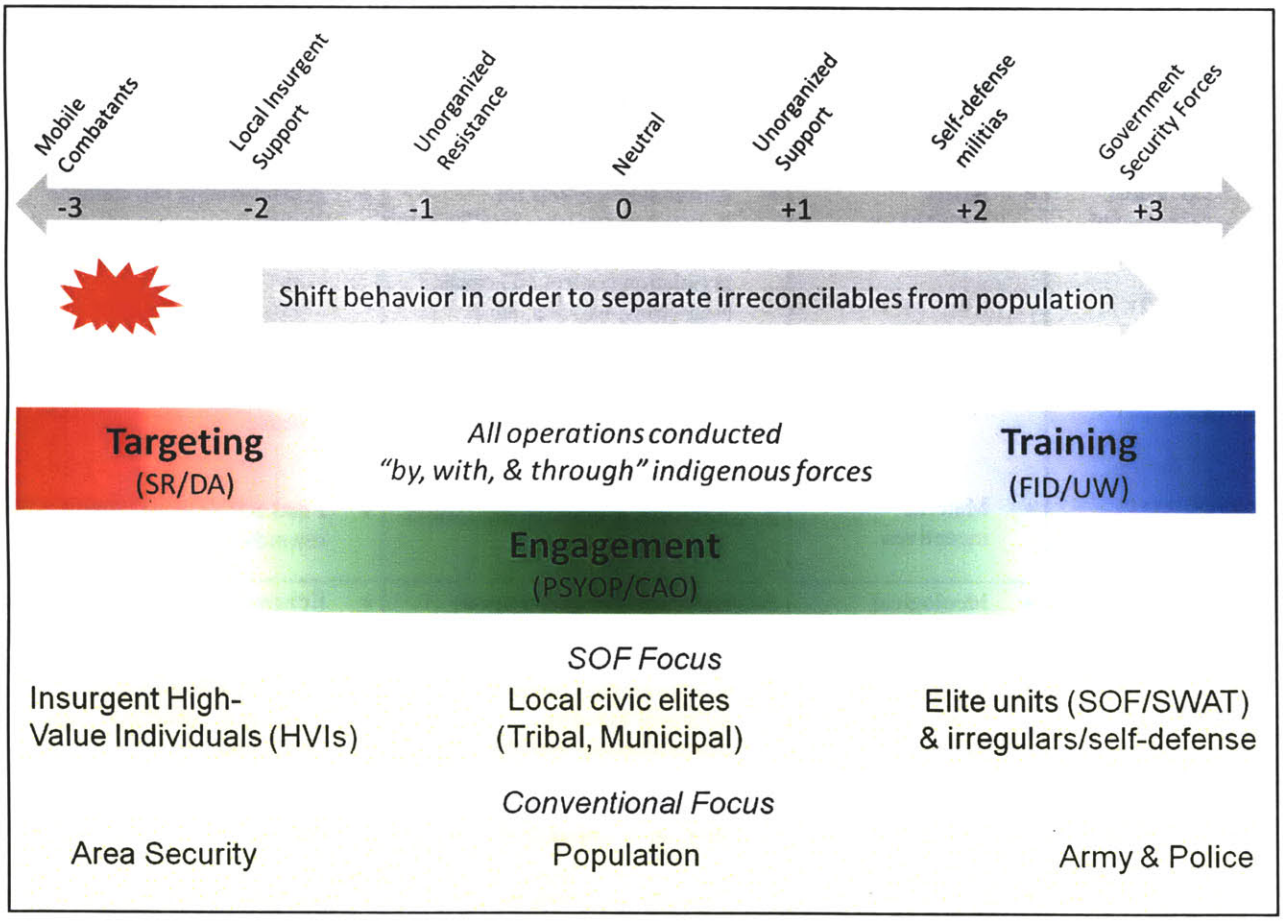


Figure 4-2: SOTF slide depicting SOF missions (from Table 5-2) in counterinsurgency.

On the negative end of the spectrum, ***targeting*** operations are military missions to selectively identify and kill or capture insurgents, emphasizing level three but also level two participants. On the positive end, ***training*** operations are designed to ensure that COIN has an indigenous face, emphasizing government forces (level three) when possible and irregular groups

(level two) when necessary. The goal of training indigenous forces is to give them an autonomous targeting capability and to avoid U.S. unilateral targeting operations (except in cases where speed and precision are critical to target a high value insurgent). Both of these are more recognizable military missions, either hunting or engaging an enemy (red forces), or training and advising indigenous security forces (blue forces) to do the same. Between them, however, is a third category of ***engagement*** operations working with the rest of the population of potential strategic actors. Neither enemy "red," friendly "blue," nor strictly speaking neutral "white," these are sometimes called "green networks" to include community, tribal, and municipal populations in the level one area.

These missions roughly cluster in three ways in Table 10-1. While PSYOP and civil affairs appear widely throughout the table (every operation has some psychological effect whether intended or not, and civilians and the expenditure of money are involved across the board), these "non-kinetic" activities are especially emphasized in row A, addressing that segment of the population responding to society-wide factors. The "kinetic" missions are respectively emphasized to deal with level two and three insurgency (col. II, rows B-D) because they represent the application of selective violence to coerce or deter insurgents (kinetic targeting is listed in row A only in a negative sense of controlling targeting errors and collateral damage). The third cluster of missions (col. III, rows B-D) emphasizes security assistance and combat advising with irregular or government security forces.

In Petersen's theory, the level-2 segment of localized support for (or against) insurgency in the form of intelligence provision, safe houses, and local armed activity, is particularly critical for insurgent mobilization; accordingly, the overlap of engagement and targeting activities is important for sorting out insurgents from the local population. Given the critical importance of local context and individual motivation in internal war, the integration of engagement with both targeting and training (at the -2 and +2 segments) is especially important. This puts the counterinsurgent in a dilemma because he must curtail local insurgent activities in order to combat the insurgency, but targeting errors and indiscriminate violence (which kill and injure zeros and ones instead of just twos and threes) can lead to more shifts to level two and further sustain those already there.

Engagement is where military forces often have the most trouble in COIN because persuasion, communication, negotiation, and alliance building are the core activities, and these are not part of regular military training regimens. Targeting and training have more demonstrable success metrics (how many insurgents killed, how many battle drills run, etc.), whereas engagement is an ongoing and ambiguous activity. Engagement operations are critical, however, because they facilitate training and targeting, often shading into them. They are the elusive link between measures of performance (what a military is doing) and measures of effectiveness (what is actually happening as a result), because engagement deals directly with the political and informational challenges at the heart of COIN. Engagement again highlights the critical importance of level two participation, on both the insurgent and militia side, because this is where the other types of COIN operations overlap. Targeting and training are mutually supportive in a relatively straightforward way because their target segments are on the far ends of the participation spectrum. The relationships with engagement, however, are far more complicated because they are situated in the problematic transition zone between level one and level two behaviors. It is risky to talk to or pay potential enemies, but when trying to stem insurgent generation and penetrate their organizations, it is dangerous not to. It is controversial to pay or train irregular forces, but when government forces are weak and unable to solve the discrimination problem, it is dangerous not to.

The Causal Linkage of COIN Missions

Figure 10-3 is based on a slide which I put together at the SOTF to show the ideal causal linkages between all of the different missions in the SOTF portfolio. Integration of all of them, in principle, helps to focus targeting on the most virulent core of the insurgency while controlling negative unintended consequences, all focused on achieving the ultimate objective of political stability (or at least enough so that U.S. forces can go home). While this appears overly complicated (and no one ever said COIN was simple), it does describe the causal relationships between and thus justifications for different missions, going beyond vague overtures to "synergize" what would otherwise be a fairly random set of capabilities.

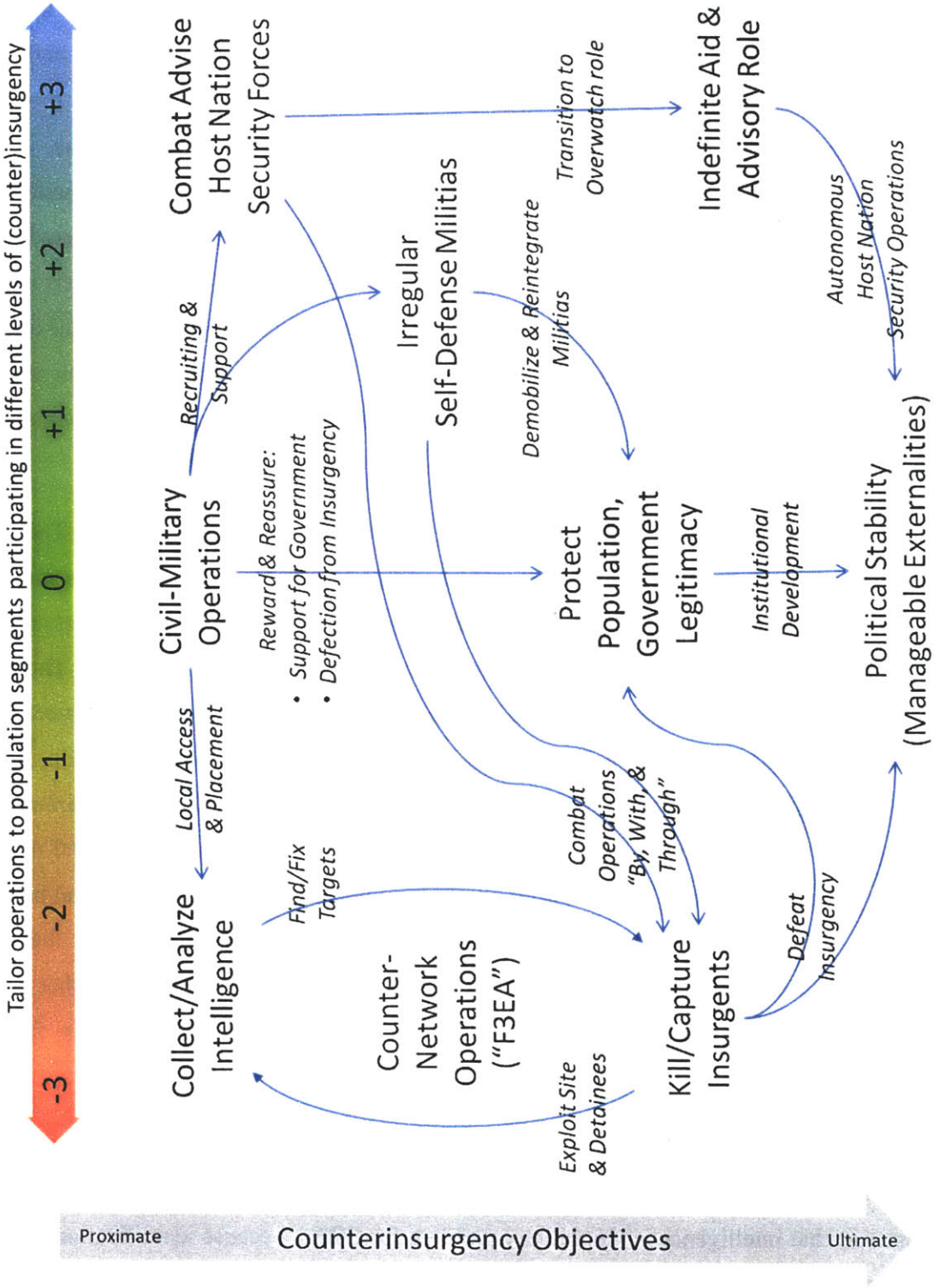


Figure 4-3: Based on a SOTF slide, displaying normative linkages between different SOTF missions

This COIN theory is not a simple template for success. Depending on the local conflict structure, the balance between the three types of operation could vary radically, and it may be necessary to emphasize some causal links over others. This should be done on the basis of a good understanding of the endogenous interaction between insurgents, militias, community networks, and COIN forces. Furthermore, there are many reinforcing and balancing feedback loops throughout this system and thus many possible paths through it. Not depicted here are a concurrent set of operations that the insurgency is also running to inhibit, counter, and subvert these linkages. This will tend to exacerbate the already noted endogenous character of civil war. What this theory does do, however, is lay out in ideal terms the relationships between different types of operations in their contribution to gradual COIN success. Implementation is an operational and circumstantially contingent art.

On the left side of Figure 4-3 is the counter-network targeting cycle. This can be a complicated cycle for militaries to get right and iterate quickly with all of the moving parts involved and the time-sensitivity of furtive human targets. Nonetheless, most eventually figure it out, using each operation to generate intelligence as a stepping stone to the next. The danger, as discussed throughout this project, is that this can become an endless do-loop subject to endless optimization on the assumption that if it only runs faster and more accurately then the "critical nodes" of the insurgency will be broken. This is remarkably similar to the airman's classic theory of strategic bombing, whereby the identification and interdiction of critical nodes in the target system will paralyze enemy operations.[7] As empirical experience with aerial bombing has rendered that theory suspect (without diminishing adherents' faith in it), so is there room to question a pure counternetwork approach to COIN. If the connections to the other operational areas (training and engagement) are ignored, the counternetwork loop can in fact become counterproductive.

It is also important to highlight the role of intelligence in this theory. If every operation has a potential PSYOP effect, so does every operation have intelligence potential. There is great consensus that intelligence is *the* military problem for COIN, because identification of insurgents (or better said, civilians who are occasionally incentivized to support the insurgency) is so hard. With high costs for targeting errors (easily marginalized with a myopic focus on running the CT

[7] See Chapter 6 and Appendix B.2: Targeting in Historical Context.

cycle faster), it makes sense to seek intelligence advantage wherever possible. Civil affairs operations come into their own here by providing an excuse to interact with the population on ostensibly benign terms, yet providing COIN forces with potential access to and placement within community networks. One such scheme used by the British in Northern Ireland involving a laundry service which tested for explosive residue, allowing for the identification of individuals in contact with someone in the bombing business.[8] Front companies have long played a venerable (some might say dubious) role in the history of espionage. There is no end of creative intelligence collection possibilities associated with civil affairs projects, meetings, and surveys, a great deal of which can even be realized completely overtly, such as through chatting up the chief of tribal security during a dinner with the tribal sheikh. While there are legitimate fears among some civil affairs personnel about being associated with intelligence, fearing for their own credibility and safety, this is simply a matter of intelligence tradecraft no more ethically or operationally difficult than other collection operations (which *always* have similar dilemmas about cover and should only be attempted by trained personnel with careful planning).

Further sources of local intelligence often neglected are the very forces being trained. Both regular and irregular personnel may be from or have family in locations that the counterinsurgent would like to gain access and placement. It is easy for COIN trainers to focus only on teaching tactical skills to their students, forgetting that each individual is a rich source of local knowledge, at least of general atmospherics if nothing more actionable. For engagement and training, moreover, the information needed to understand local politics and events is noisy and relatively available for overt collection if personnel are out amongst the people; this contrasts greatly with the expensive, perishable, and often technical intelligence needed to support targeting missions. A further reason to overlap training, engagement, and intelligence operations is that every foreign contact, very much including students being trained for combat, is also a counterintelligence liability.

Civil affairs (and PSYOP) is also useful in support of training efforts. Standing up self-defense groups is a tricky business, and it is necessary to work with local elite to provide reliable men and enforce norms of operation, less the militant treatment become worse than the insurgent

---

[8] Martin Dillon, *The Dirty War: Covert Strategies and Tactics Used in Political Conflicts* (London: Hutchinson, 1990), 27-61.

disease. It is also important to integrate security forces and the population they protect, or at least try to diminish the level of dysfunction between them. The police in Baathist Iraq, for example, were an abusive gang of thugs greatly feared by the people; there was no concept of "the thin blue line" "to serve and protect." A way to start changing this is through involving partner security forces in humanitarian assistance, literacy programs, and development activities in order to build bonds of trust between security forces and the people, with the positive benefit of a greater willingness of the latter to inform on insurgents. Like combat operations, civil affairs projects should be conducted "by, with, and through" locals.

The ultimate objective in Figure 10-3 is not victory, per se, but getting the negative externalities of the conflict down to a manageable level consistent with U.S. interests. Thus insurgent groups may not be decisively beaten, but only whittled down and contained. Furthermore, from a SOF perspective, training engagement does not cease, but downsizes into a training initiative managed through the American diplomatic mission. Whereas the height of engagement may see SOF combat advising indigenous security forces, leading them on dangerous combat missions, the goal is to transition into an overwatch role providing operational advisement only during emergencies, and then into simply a stand-off training role. The demobilization and integration of irregular forces into legitimate civilian or government employment can be especially challenging and is doctrinally recognized as the hardest phase of UW; it also not, strictly speaking, necessary as long as their activities are not exacerbating the very conflict they were leveraged to suppress. Because unconsolidated and dysfunctional governance is at the root of many civil wars, addressing this goes well beyond military problem of abating insurgent violence and may be beyond the capacity and will of the U.S. government to address in every case. While the consolidation of government monopolies on force is a long term process, it is desirable to remain involved in at least some minimal capacity with both FID and UW partners in case the conflict reignites and also to maintain intelligence situational awareness.

To sum up so far, following from Petersen's description of the social mechanisms which trigger and sustain insurgency, the basic thrust of COIN is to inhibit these mechanisms and promote counter-triggering mechanisms in the other direction. Doing this involves conducting three different but interdependent types of operation—targeting, engagement, and training—

focusing on different segments of the population, with attention especially to the overlap around the level two segments. The basic objective of COIN is to shift popular behavior away from the insurgency in order to separate (identify and target) irreconcilable elements, and this is done by conducting targeting, engagement, and training operations by, with, and through indigenous groups to try, as much as possible, to maintain local ownership of the conflict.

SOF and Conventional Forces in COIN

While I have used SOF missions to describe particular operational concepts, this has been intended as a more general re-theorizing of COIN in terms of causal mechanisms from civil war theory. In COIN conventional forces are actually performing SOF missions, but at a larger scale. The theoretical linkages between them should be the same. In a large scale COIN effort where conventional forces are the main effort, SOF are employed in specialized niches in each type of operation, but both types of forces do in fact conduct targeting, engagement, and training.

The distinctions sketched out here are very much an ideal ones, but they follow from the different scale of the two kinds of forces. SOF, small and specialized by design, focus on those aspects of local networks where they can get the most leverage. For insurgent networks, this means identifying insurgent leaders, administrators, facilitators, and other high valued individuals, conducting targeting operations to kill or preferably capture them when intelligence triggers are met. By contrast conventional forces focus on area security, which may involve large scale operations (as in Fallujah in 2004), but routinely involve regular patrolling and population control which SOF can't do other than through indigenous partner forces. Likewise for training, whereas conventional forces focus on developing general army and police forces, SOF are integrated with smaller specialized units which are trained to a higher level of proficiency, or with irregular units that must be handled with more discretion. The distinction in engagement is far vaguer, but the principle of leveraging "high value individuals" in the "green network," rather than reaching out to the entire local population, is similar. The vagueness with engagement stems from the fact that conventional "battlespace owners" have far more negotiating resources and persistence in local areas, and so of course interact frequently with local elite, with SOF focusing on different (perhaps more sensitive, controversial, or neglected) networks. Conventional CAO, furthermore, is generally focused on development, reconstruction, and governance, whereas SOF projects are more focused means to an end. The

actual employment of both types of forces worked out in practice and is likely to deviate substantially from these ideal distinctions.

A more complete discussion of SOF and conventional force integration is beyond the scope of this discussion,[9] which aims simply at sketching out a theoretically-grounded integration of the different SOF capabilities employed in COIN. A broader discussion would also have to consider the conditions under which the small-scale SOF-only approach to COIN is more or less appropriate than a large-scale conventional effort. I have argued that both approaches should involve conduct the same three generic types of operations, with similar causal relations between them. The scale of the COIN effort, however, is a huge question with major implications for the endogenous dynamics of the conflict. The first casualty of scaling up is likely to be the "by, with, and through" clause as the conventional force takes on more and more COIN responsibilities itself.

This discussion has also completely left aside consideration of interagency contributions and general political coordination of the entire COIN effort. Given that COIN is largely a state building problem, these are widely recognized as major overarching requirements of an overall intervention strategy, and integrating them a major US policy challenge.[10] From the present theoretical perspective, nevertheless, it is possible to view these in terms of engagement operations writ large, scaled up to include activities of the State Department, USAID, NGOs, etc. Any strategic coordination of all the instruments of national power for the COIN effort would still have address the triggering and sustaining mechanisms of insurgency by promoting inhibitory and counter-triggering mechanisms through engagement, training, and targeting operations. While I have described this on the smallest scale possible, as an integration of SOF capabilities, a much more scaled up and complex COIN effort would have the same basic structure. The devil is in the details of implementation.

---

[9] See Gary Luck and Mike Findlay, "Special Operations and Conventional Force Integration," United States Joint Forces Command, Joint Warfighting Center, Focus Paper no. 5 (2008); US Special Operations Command Pub 3-33, *Conventional Forces and Special Operations Forces Integration and Interoperability Handbook and Checklist* (MacDill Air Force Base, FL: 2006); Joseph D. Roller, "Leaders Wanted: SOF and CF Integration," Air Command and Staff College Paper (2006).

[10] David C. Gompert, John Gordon, Adam Grissom, David R. Frelinger, Seth G. Jones, Martin C. Libicki, Brooke Stearns Lawson and Robert E. Hunter, *War By Other Means: Building Complete and Balanced Capabilities for Counterinsurgency, RAND Counterinsurgency Study, Final Report* (Santa Monica, CA: RAND Corporation, 2008)

Note that the institutional bias in US SOF toward commandos (targeting) at the expense of advisors (training) and diplomats (engagement) couldn't come at a worse time. Insofar as civil and irregular warfare has a dismally promising future in the twenty-first century, American interventions must involve a nuanced balance of targeting, training, and engagement operations. Because these wars take time to resolve, and do so rather ambiguously, it is preferable to be able to manage them with smaller more discrete investments, rather than have to go through painful cycles of COIN learning with large deployments. This is not possible, however, without a cadre of operators who are adept at the advisor and diplomat roles as well as the commando. An imbalance could be quite counterproductive. It is important for the "quiet professionals" to talk to the locals, even if, or especially because, they will probably end up killing some of them.

Appendix C: A Transaction Cost Theory of Information Friction

Information friction theory as presented in Chapters 3 and 4 is scoped to explain any sort of military command and control, but its relevance should be more generalizable to to any sort of information system, military or civilian. My discussion in Chapter 4 was inspired by a political economy concept of information friction in terms as the strengths and weaknesses of decentralized markets and hierarchical regulation: (1) market efficiency or expedient adaptation; (2) regulatory efficiency or enterprise integration; (3) market failure or mutual interference; (4) regulatory failure or bureaucratic insulation. These four fundamental ideas can be related through the idea of basic *transaction costs* in any information system: (i) costs of communicating information; (ii) costs of adapting information systems.

Table 10-2: Information friction as a function of information system transaction costs

	Low Adaptation Costs	High Adaptation Costs
High Connection Costs	Expedient Adaptation	Bureaucratic Insulation
Low Connection Costs	Mutual Interference	Enterprise Integration

In Chapter 4 I tried to avoid excessive abstraction in an already long and complex project, so I presented three familiar levels of analysis (structure, organization, individual) of direct causes of information friction. I actually believe that those causes matter because they shape these two basic transaction costs, which gives rise to the four different configurations of information friction as market/regulatory efficiency/failure in knowledge management. I present this background thinking here as a stepping stone for future work, as well as to document a stepping stone in the historical development of the theory presented in Chapter 4.

Theoretical Precedents

I will first describe the very different sources of the basic logic in Table 10-2 before fleshing out its ideas a bit more. While these terms are perhaps non-intuitive, the concept appears in other places. I believe that many different scholars have been pointing out some basic constraints on any sort of information system as they analyze their own specific kinds of information systems: monetary policy, corporate innovation, and organizational rules. I will sketch out a synthesis.

Monetary Trilemma

The original inspiration for my model—which describes any information system—is the "impossible trilemma" of macroeconomic monetary policy. Central banks would like to achieve three goals: fixed exchange rates, domestic policy autonomy, and international capital mobility. Unfortunately, they can at best only achieve two of three: the gold standard sacrificed domestic autonomy; Bretton Woods constrained capital mobility; the present floating exchange rate regime undermines exchange rate stability.[1] Table 10-3 shows this trilemma as a 2x2 matrix listing three possible monetary regimes (in bold) that each take two of three of the desirable properties, plus a fourth category of inefficient regimes that take only one or none; this is shown as a table to highlight the logical similarity to Table 10-2 and the other theories reviewed below.

Table 10-3: Macroeconomic trilemma

	Domestic Monetary Autonomy	International Coordination
Capital Controls	**Fixed Exchange Rate** (Breton Woods)	Inefficient whether exchange rate is fixed or floating
Capital Mobility	**Floating Exchange Rate** (Contemporary system)	**Fixed Exchange Rate** (Gold Standard)

We should be able to generalize the monetary trilemma as a specific instance of a more general constraint on any sort of information system. The *referential integrity* of money (its "meaning" or "truth") is its usefulness for exchange, and people desire that value to remain stable in order to be able to cash it in for real goods. Control of domestic policy is a form of *local institutional adaptation* to maintain this stability. International capital mobility requires *efficient connection* with other economies to be able to use this money for valuable exchanges with goods that are far away. We thus have the stable reference of the representation, the local adaptation of the information system, and the connection of the information media with remote entities. Any information system can maximize at most two. Local initiative foregoes connection. Mutual interference forgoes stability. Enterprise integration forgoes adaptation. Bureaucratic insulation is the most inefficient, forgoing both connection and adaptation in the quest for stability.

---

[1] Maurice Obstfeld, Jay C. Shambaugh and Alan M. Taylor, "The Trilemma in History: Tradeoffs Among Exchange Rates, Monetary Policies, and Capital Mobility," *Review of Economics and Statistics* vol. 87, no. 3 (2005): 423-438; Barry Eichengreen, *Globalizing Capital* (Princeton University Press, 1998); Dani Rodrik, "How Far Will International Economic Integration Go?" *Journal of Economic Perspectives* vol. 14, no. 1 (2000): 177-186.

User and Firm Innovation

Another inspiration for Table 10-2 is Eric von Hippel's work on user innovation, which Chapter 3 discussed in the section on expedient adaptation. Von Hippel, like other proponents of peer production, champions bottom-up open-source designs over careful top-down management of innovation by firms. But this is a conditional tradeoff. Carliss Baldwin and von Hippel describe a model of firm and user innovation in terms of communication and design costs.[2] Their model says nothing about the case where both types of costs are high, but this can be considered the regime of government provision of public goods (*e.g.*, canals, railroad surveys, and interchangeable machine parts in the nineteenth century, or radar, satellites, nuclear power, and the internet in the twentieth), which are often innovative but very difficult to manage.

Table 10-4: The source of innovation as a function of design and communication costs

	Low Design Costs	High Design Costs
High Communication Costs	Single User Innovation	No innovation or government innovation
Low Communication Costs	User and firm innovation are viable and compete	Firm innovation (at an extreme of both costs, open-source dominates)

The strange overlap in the high design, low communication cost box in Table 10-4 speaks to the interdependence of regulatory frameworks and decentralized efficiency. Markets require institutional structure in order to function at all. Large-scale open source projects can only work when they find a way to solve the integration problem, which in essence defines a modular architecture that allows single user innovation to flourish within defined sandboxes. The transaction costs Baldwin and von Hippel describe in Table 10-4 are very much the same as I describe in Table 10-2

Practical Drift

A third inspiration for Table 10-2 is Scott Snook's theory of practical drift, which describes a dynamic perspective on how distributed organizations move through different

[2] Carliss Baldwin and Eric Von Hippel, "User, and Open Collaborative Innovation: Ascendant Economic Models," Harvard Business School Finance Working Paper 10-038, 2009

configurations of system coupling and adherence to formal rules.[3] Organizations formulate explicit SOPs to coordinate units (tight coupling, rule-based logic), but this drifts into unstable insulation as units become distributed (loose coupling, rule-based logic), which then provides space for local actors to deviate from SOP to informally optimize (loose coupling, task-based logic), which then heightens the risk of accident and fratricide—Snook was motivated to explain the 1994 Blackhawk shootdown in Iraq—when units with divergent expectations about each other collide (tight coupling, task-based logic). Table 10-5 shows the "practical drift" through different states of system coupling and rule adherence, numbered according to their dynamic sequence.

Table 10-5: Practical drift

	Task-based Logic of Action	Rule-based Logic of Action
Loose System Coupling	3. Local variations thrive in a stable system	2. Cumbersome rules are difficult to enforce
Low Communication Costs	4. Accidents are likely in this unstable system	1. Standard operating procedures stabilize the system

The dynamic cycle in Table 10-5 maps Table 10-2 to the concept of the endogenous growth of information friction in 0. These are three very different theories from three very different backgrounds. The fact that they appear—as I have laid them out in Table 10-3, Table 10-4, and Table 10-5—to be getting at some of the same ideas prompts the general notion of information transaction costs in Table 10-2 which should apply to any information system, military, economic, government, corporate, or social. We should expect this to be the case, for as emphasized throughout this project, IT is a fundamentally intermediate and pervasive presence in anything a human organization wants to do.

Information System Transaction Costs

Information makes both cooperation and competition possible, and the institutions which stabilize information channels have technical as much as normative foundations. My synthesis is thus consistent with Douglass North's argument that socioeconomic institutions arise to respond to the transaction costs of monitoring and enforcing contracts, which is a highly informational

[3] Scott Snook, *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks over Northern Iraq* (Princeton: Princeton University Press, 2000). Snook draws heavily on Charles Perrow, *Normal Accidents: Living with High Risk Technologies* (Princeton, NJ: Princeton University Press, 1999).

activity: "Information processing by the actors as a result of the costliness of transacting underlies the formation of institutions."[4]

Advances in IT have both centralizing and decentralizing tendencies because IT tends to lower two basic types of transaction costs associated with institutional control. IT lowers *connection costs* through physical connectivity and logical protocols that improve communication and coordination between entities that are distributed in time and space. IT lowers *adaptation costs* by making it easier for actors to tailor information systems to their local computational problems, most obviously by reconfiguring software settings without having to buy new hardware. Historically, these two functions are rooted in the dual inheritance of modern IT: communication and computation systems. Communication is the classic category, which includes telegraph, telephone, and radio. Computation for scientific calculation, industrial control, and office administration has developed in parallel but especially with the more recent profusion of digital IT. The line between communication and computation is largely blurred in the present age of pervasively networked machines (*i.e.*, communicating computers). The dual regulatory systems institutionalized in government communication policy make for ongoing controversy around IT.[5]

---

[4] Douglass C. North, *Institutions, Institutional Change, and Economic Performance* (Cambridge University Press, 1990), 107

[5] European writers tend to use the term Information and Communication Technology (ICT) where Americans just use IT. Oettinger coined the term "compunications" to describe the historical merger & emerging regulatory challenges: Anthony G. Oettinger, "Compunications in the National Decision-Making Process," in *Computers, Communications and the Public Interest*, ed. Martin Greenberger (Baltimore MD: Johns Hopkins University Press, 1971): 73-114. A good overview of IT regulatory politics in the context of this dual inheritance is: Gerald W. Brock, *The Second Information Revolution* (Cambridge, MA: Harvard University Press, 2003).

Table 10-6: Basic information system transaction costs

	Connection Costs	Adaptation Costs
Practical function	Use	Design
Intentional focus	Content: control the world; entities, properties, events, values on variables	Format: control representation; architecture, methodology, definition of variables & models
Scope of control	Across groups	Within group
Historical IT function/domain	Communication	Computation
Cause célèbre of modern IT	Connect people in a global village; shrink space and time; rationalize management	Empower people to access powerful tools & creatively tailor local solutions
Representational qualities that lower costs	Communicable, Commensurable, Panoptic, Impersonal, Abstract, Quantifiable, Secure	Accessible, Understandable, Configurable, Extensible, Personalizable, Combinable, Supported, Testable

We can analytically distinguish these two types of transaction costs because they have different effects. Declining costs of connection make it possible to broadly share standardized data, which will have a centralizing effect by empowering hierarchical control. Declining costs of adaptation make it possible for smaller-scale actors to align their own data management with salient environmental features, which will have a decentralizing effect by empowering local actors. Lower connection costs promote the widespread and stable *use* of IT, while lower adaptation costs facilitate IT *design*. The convergence of communication and computation functions in the historical evolution of the IT field helps to explain the substantial blurring between IT use and design. All else being equal, technical improvements can enhance connection and/or adaptation. These qualities have conflicting effects on information system behavior in terms of good decentralization (where local adaptation is improved) and good centralization (where organizational standardization is improved). The unstable contrast between them creates potentials for bad decentralization (where adaptation is dangerously uncoordinated) and bad centralization (where high coordination costs make it hard to get anything done). Since IT itself is indeterminate on organizational control, the management of the competing effects requires additional, complementary organizational action (policy, norms, enforcement, subversion, *etc.*) to raise and lower these costs beyond the contribution of technology alone.

Layers of Connection and Adaptation

To keep the concepts of connection and adaptation analytically distinct, it is important to recognize that a group is recursively composed of other groups: adapting IT *within a group* actually involves connecting *elements of that group*. In Figure 10-4, small groups of people and IT (documents, code, databases) connect and coordinate their behavior in order to adapt their local situations. The small groups themselves in this picture form higher order groups which may or may not have to coordinate closely with other groups.

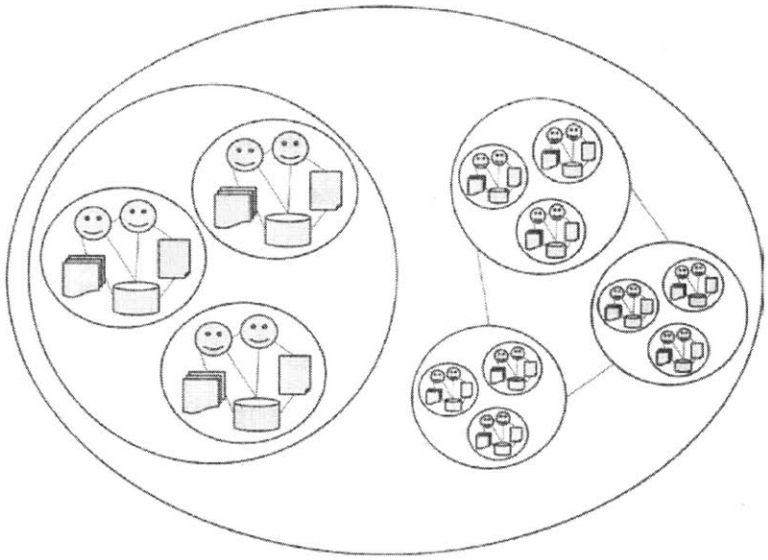


Figure 10-4: Groups are recursively composed of other groups

The adaptation of IT within a group at one level of analysis involves the connection via IT across the members of that group. This adaptation at the group level requires that those group members are not themselves adapting. When IT components are stable, it is possible to use them as a combinatorial foundation for new ones. The rationalizing qualities of connective IT (commensurable, abstract, quantified, *etc.*) are the opposite of the qualities of situated reality (unique, material, chaotic, *etc.*), and the process of IT adaptation is the process of making local reality *less messy, more understandable, and more manageable.* Adaptation is information system design, which may be more or less *ad hoc* depending on technical skills, using locally available resources to rationalize local processes.[6]

[6] For instance, if I have some digital photographs, the tracklog from a handheld GPS receiver I carried with me when the photos were taken, a software mapping package, and a few lines of custom code, then I can correlate the timestamps on the images with the time on the tracklog to associate geographic coordinates with the images,

Multiple actors can create centers of calculation where inscriptions of events further away in space and time are gathered together. The use of IT exerts a centralizing effect on the local institutional components that actors can access, but it can have a decentralizing effect across a set of actors since each is enhancing their own control. Because IT can amplify power for multiple actors, these networks become subject to corruption and compromise through competition and interference. Actors use IT to centralize, standardize, and extend their distributed cognition; yet because they compete for influence, they collectively end up with decentralized and messy interactions. This just shifts us back into the balance of power among organizations (or organizational subunits).

Groups—which are composed recursively of smaller groups of people and IT—can either move collectively toward overall mission effectiveness or work at cross purposes with different concepts of effectiveness. Thus in the box at the top left of Figure 10-5, the three systemically independent groups pictured are each exercising local initiative in order to achieve lower-order enterprise integration among their group members: arrows in the same direction indicate contribution to public welfare; the magnitude of arrows indicate ease of adapting/designing IT; solid lines indicate stable connection, while dotted lines indicate difficult, costly coordination.. IT and organizational policy determine adaptation and connection costs, with different consequences for information system behavior. IT usage thus promotes centralization by lowering connection costs and making enterprise integration feasible, but also decentralization by making adaptive design feasible for smaller scale actors who can take local initiative.

---

so that I can plot icons of their locations on a map. In doing so I am communicating to my computer quantified datafeeds that I combine into an abstract, panoptic representation of my recent photographic activity. The result is a novel adaptation for me and my tools (my group) that didn't exist before and which depended on my knowledge of how to use these tools and how I wanted to use them in my local activity. This representation makes my past photographic activity visible and I can use it to further structure my activity, such as easily identifying the places where I haven't taken pictures and might want to visit in the future. There are now cameras on the market with GPS receivers built in which obviate the need for this sort of hack, but hopefully the example is illustrative.

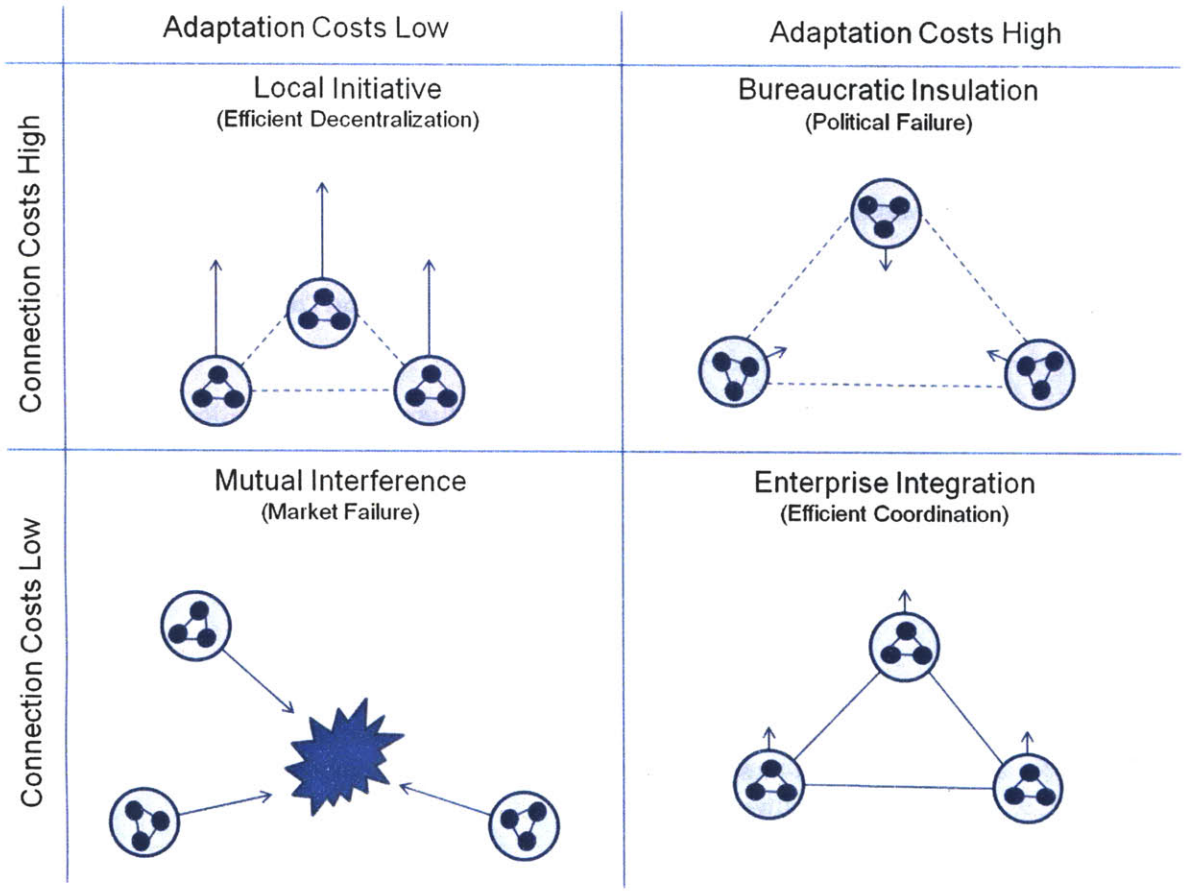


Figure 4-5: Graphical depiction of information friction as a function of connection and adaptation

It's important to bear in mind that, while technical advances in IT tend to lower both types of cost, organizational actors also have other means—persuasion and coercion—to alter costs in order to protect their political interests within the organization. Organizations can also affect costs through manipulating authority relations, informal norms, economic incentives, *etc.* For example, fragmentation in the organizational environment might raise connection costs regardless of what sort of IT is in play. Alternately, an organization might want to raise adaptation costs by prohibiting users from installing and running software that the IT department has not tested and approved. Thus while there is a natural tendency of emerging IT to move communities toward mutual interference (where both types of costs are lowered), the embeddedness of IT in social life means that actors seek to actively manipulate these costs through whatever means at their disposal. Bureaucratic insulation (where both costs are higher), is a common result of policy overreaction to interference problems. Any particular cases are dependent on organizational politics

Basic Tradeoffs in Information Systems

Figure 4-5 and Table 4-7 (a more detailed version of Table 4-2) summarize the four ideal categories of information system behavior *within a given level of analysis*.

Table 4-7: Characteristic Information System Tradeoffs

	Adaptation Costs Low	Adaptation Costs High
Connection Costs High	**Local Initiative (or Expedient Adaptation)** "Good decentralization" • User innovation • Responsiveness • Self-Organization	**Bureaucratic Insulation** "Bad centralization" • Work-to-Rule Slowdown • Rent-seeking • Lock-in
Connection Costs Low	**Mutual Interference** "Bad decentralization" • Non-Interoperation • Negative Externalities • Adverse Selection	**Enterprise Integration** "Good centralization" • Economies of Scale • Standardization • Accountability

Any organization would like to have both decentralized initiative and centralized integration in order to bring representational structure into coordination with environmental structure. The only way to square the circle is to manage the different layers of the information system with different modes of control and to coordinate them with different features of the environment. The layers of abstractions which characterize IT architectures enable this partition of command, but it also means there are many opportunities for personnel to intervene for better or for worse in the attempt to coordinate internal and external structure. Any given balance has inherent risks of too much order and too much chaos for each layer. The pace of change in IT use and design, furthermore, which involves the proliferation of abstraction layers and modules which actors can exploit and recombine, is likely to exacerbate these risks by complicating the balance.

Table 4-8: Dynamic relationships between transaction costs

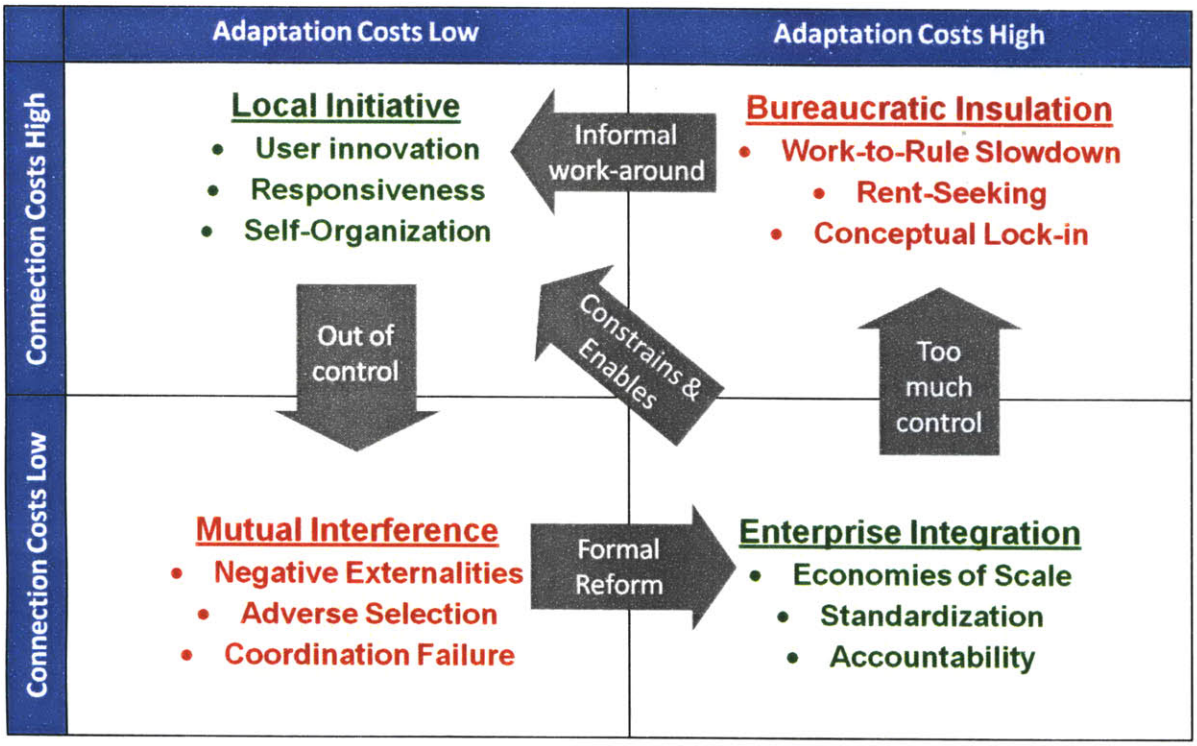


Table 4-8 shows the typical movement around these tradeoffs as organizations work through them, struggling to balance the strengths and weaknesses of markets and hierarchies at different levels of analysis. The tradeoffs are like those of the monetary trilemma, but more dynamic since so many actors are involved in the "domestic policy" of their own IT interaction. The dynamic patterns trace a pattern something like what Snook describes in practical drift. The relationship between integration and initiative is basically that between efficient regulatory institutions and free markets.

Table 4-9: Military examples of different configurations of transaction costs

	Adaptation Costs Low	Adaptation Costs High
Connection Costs High	**Local Initiative** • **User innovation** – Field expedients: IEDs, radar-directed naval gunfire, *PowerPoint* ersatz databases – *FalconView,* MS *Office* applications • **Responsiveness** – Nelson at Cape St. Vincent & Copenhagen; turning off radio, taking creative license – Reformatting for interoperability • **Self-Organization** – OEF "Afghan Model," JSOC CT – Operation Michael, armored breakthroughs	**Bureaucratic Insulation** • **Work-to-Rule Slowdown** – Somme, Paschendaele timetables – Mission Planning Systems (JMPS/TAMPS) – Strategic forces C3I (Blair 1985) • **Rent-Seeking** – Politicized stats (Andreas & Greenhill 2010); Vietnam metrics (KIA, OB, HES); Polaris PERT – Gold-plating, rqmts creep, follow-on imperative • **Lock-in** – Kosovo targeting, COIN whack-a-mole, Jutland – I&W failure: 9/11, Pearl Harbor, Yom Kippur
Connection Costs Low	**Mutual Interference** • **Negative Externalities** – Insecure networks, unreliable software – Disorganized/corrupted common files & DBs • **Adverse Selection** – Information overload – Plagiarism, provenance loss, quality-control – Veracity bubbles (Iraq WMD intel) • **Coordination Failure** – C2: Mayaguez, Grenada, Eagle Claw, SNA – Collateral damage: Chinese Embassy – Fratricide: Blackhawk shootdown, L. McNair	**Enterprise Integration** • **Economies of Scale** – Systems Integration: B2, Polaris, MX – USN ASW (OSIS), Battle of Britain IADS – Bletchley Park, COIN Biometrics • **Standardization** – GPS – USN Link 16 & JOTS, Radio Prowords – Internet/COTS • **Accountability** – Blue Force Tracker – Collateral Damage Modeling

Table 4-9 shows a few examples of these states from military history, but it's important to bear in mind that even these examples will be mixed at different levels of analysis. I picked cases that seemed to especially exemplify or get stuck in the different cases.

The Relationship between Causes of Friction and Transaction Costs

I mentioned at the beginning of this appendix that Chapter 4 omitted discussion of transaction costs for simplicity of exposition. I described the three causes of information friction, but I was a little bit vague about how the different styles of information friction emerged

and interacted. Figure 4-6 depicts information friction theory with the transaction costs included. The part in the dashed box is the information system of the organization, described in the tradeoffs above.

This appendix has presented a rather impressionistic sketch of how, with political economy concepts, information friction theory can be used to analyze any sort of information system. Indeed, if human cognition is distributed as Edwin Hutchins and others argue, then we should expect it to be afflicted by political problems of coordination and conflict among all the different sociotechnical components.

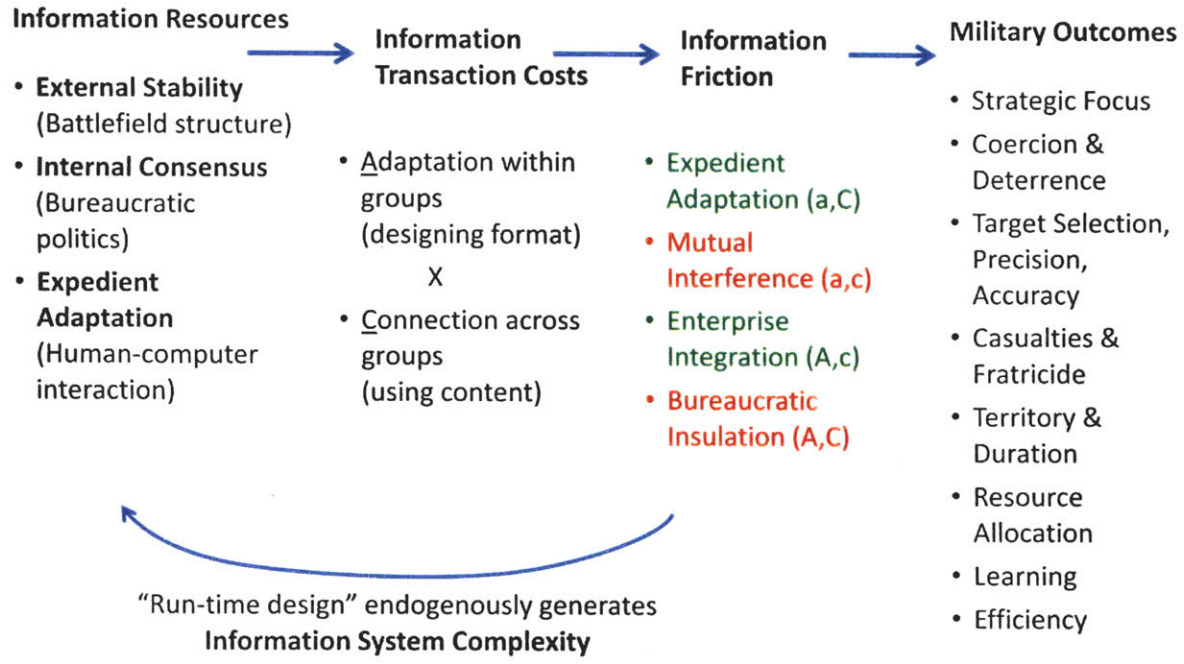


Figure 4-6: Information friction theory, including transaction costs

Appendix D:Endogenous Growth of Information System Complexity

My account of information friction in these pages has tended to emphasize its enduring and eternal quality: where there is war, there is information friction. But it's important to also recognize that the conduct of war has changed with the adoption of more sophisticated IT. The change over time creates more tangled and complex manifestations of information friction for all the personnel in the integration phase of command and control. As organizations work through fundamental tensions between hierarchical management and decentralized community based modes of information processing, their solutions to existing problems create new problems. Over time, information friction acts like a complexity ratchet for a control-seeking organization: more layers, modules, symbols, distinctions, network policies, normative constraints, working groups, coordination meetings, training programs, *etc.*

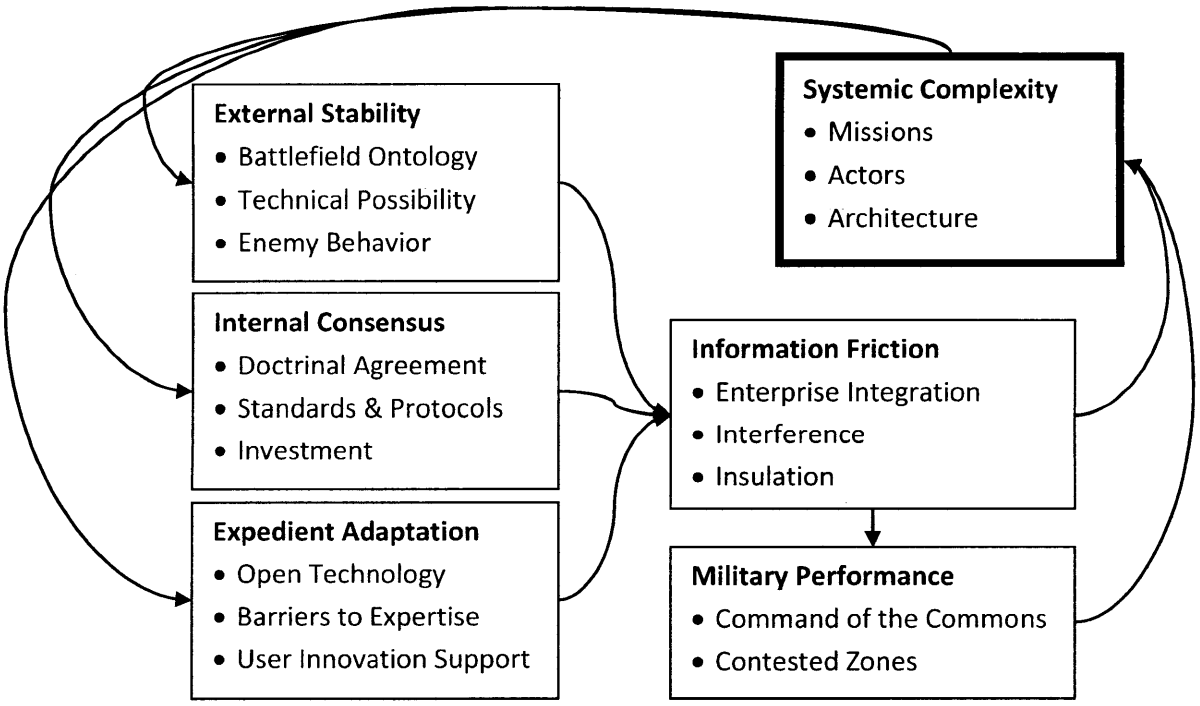


Figure 10-7: Systemic complexity as cause and consequence of information friction

Increasing systemic complexity of organizational missions, the actors involved, and the IT architecture is both a cause and consequence of information friction. Figure 10-7 diagrams

this endogenous complexity-increasing dynamic. Table 10-10 summarizes some tentative hypotheses on the endogenous growth of information friction in military organizations over time.

Table 10-10: Hypotheses on Endogenous Growth of Information Friction

EG1.	Internal consensus and external stability leads to enterprise integration (low friction)
EG2.	Internal consensus without external stability leads to insulation (high friction)
EG3.	Lack of internal consensus without runtime design leads to interference (high friction)
EG4.	Lack of internal consensus and/or lack of external stability with runtime design enables local initiative to lower information friction
EG5.	Over time, runtime design generates interference friction, which encourages organizational authorities to pursue enterprise integration
EG6.	Over time, the pursuit of enterprise integration generates insulation friction, which prompts working personnel to pursue runtime design
EG7.	The canonical permutation of information friction over time is: runtime design initiative → decentralized interference → enterprise integration → centralized insulation → runtime design workaround → *ad infinitum*...
EG8.	The canonical struggle generates more internal complexity of layers, modules, interactions, functional types, and cross-functional dependencies in the entire sociotechnical system
EG9.	Advanced intelligence and precision strike technologies improve perception and articulation phases of control, but integration becomes a serious "reverse salient"
EG10.	Division of military labor increasingly emphasizes knowledge work, so more personnel more of the time—with IT thoroughly embedded in their experience—must cope with high friction
EG11.	The proliferation of sophisticated IT throughout the commercial/civil environment complicates external stability by introducing new types of political actors and interactions
EG12.	The proliferation of sophisticated IT throughout the commercial/civil environment complicates military internal consensus about standards and protocols
EG13.	Militaries with complex information systems pursue more complicated, tangled, difficult-to-evaluate means-ends chains
EG14.	Militaries with complex information systems pursue control of the environment at greater scales and with greater fidelity
EG15.	Complicated and ambitious missions generate high friction, both interference and insulation

Appendix E: Coordination of Feedback in Distributed Control

Feedback in distributed cognition, described in chapter 3, is follow on perception after articulation in any control cycle. In military command and control, it involves using intelligence sensors to establish connection with the target environment and cascades of inscription to move collection records into disconnected centers of calculation. In the counter-network targeting example, disconnected fusion enables subsequent reconnection either as follow-on intelligence collection or as a kill/capture assault.

1. The intuition of targeting as a matter of arranging connections from a disconnected position can be developed through considering increasingly complicated variations on the problems a sharpshooter might encounter. Figure 4-8A-D and Figure 4-9 graphically summarizes these progressive variations.
2. In the basic situation, a shooter aims at a stationary target within his range. He is visually connected—in fact, they are physically connected by a column of electromagnetic energy—and need only aim and fire.
3. The target moves along a straight line. The shooter and target remain visually connected as the shooter follows the movement through a simple servo mechanism, leading the target a bit.
4. The target moves behind a tree but continues in the straight line. The visual/physical connection is interrupted, but the shooter continues to track where it *would be*, a sort of dead-reckoning in order to reconnect visually when it emerges.
5. The target changes its path behind the tree. The shooter then changes position to peer behind the tree to reacquire connection.
6. The shooter loses the erratically maneuvering target behind many trees. His dead reckoning fails to maintain reference to the target. Other hunters, however, make visual connect with the target. They transmit their sightings and locations via radio, another physical connection. The shooter marks records of the sightings on a map to triangulate the target and figure out where to move to get a shot. The observers cue the shooter to relocate and reconnect with the target.

In each case the shooter has to adjust his gaze, compensate for his own movement, and stabilize his representation of the target, the movement of which is constrained as a physical entity in the world. The shooter's goal is to connect a bullet with the target. The problem is that the shooter becomes disconnected from the target. Yet this very disconnection provides him the

space to adjust, compensate, and stabilize his own representational structure in order to enable reconnection.

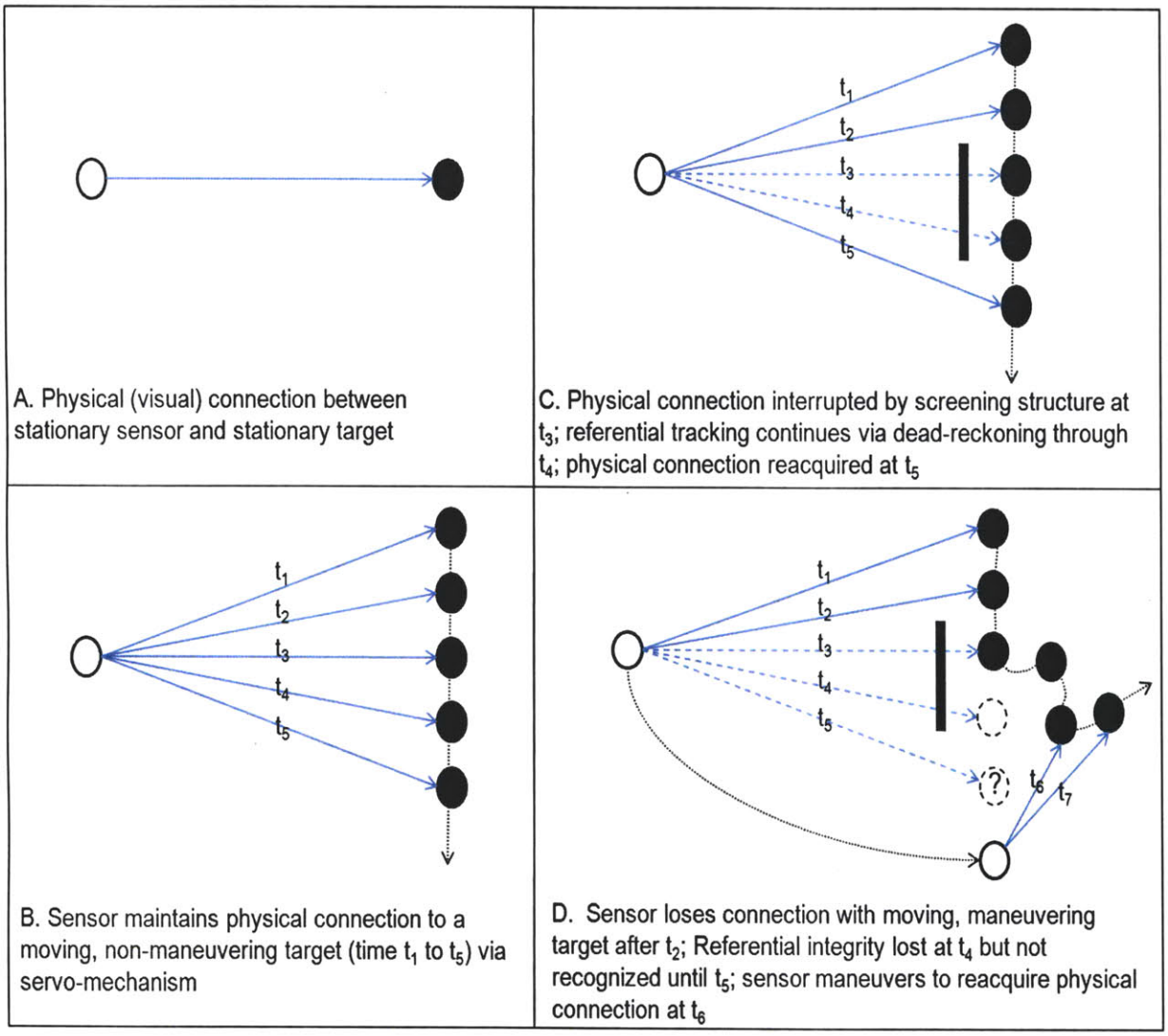
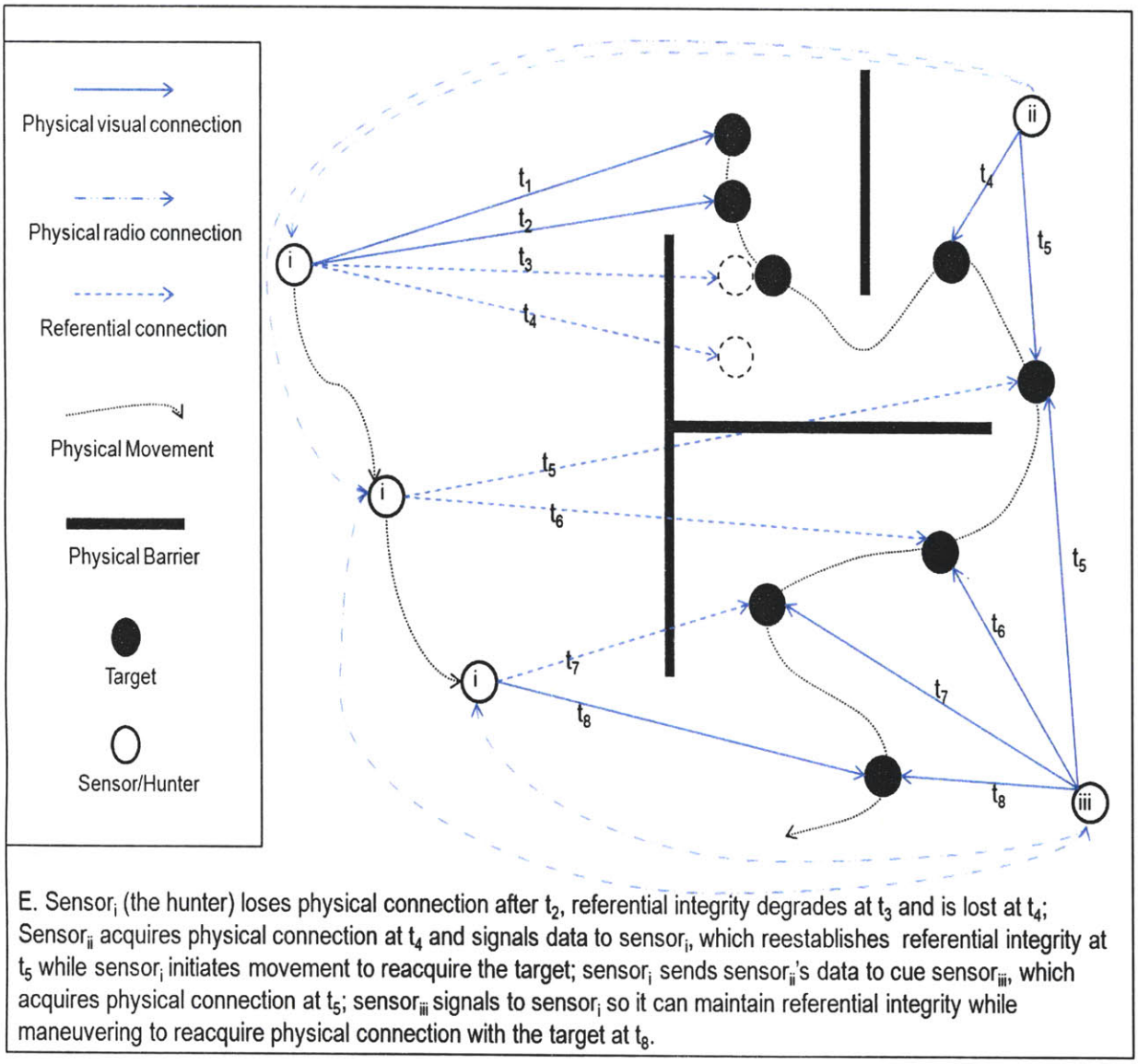


Figure 4-8: Progressively more difficult problems of maintaining reference



E. $Sensor_i$ (the hunter) loses physical connection after t_2, referential integrity degrades at t_3 and is lost at t_4; $Sensor_{ii}$ acquires physical connection at t_4 and signals data to $sensor_i$, which reestablishes referential integrity at t_5 while $sensor_i$ initiates movement to reacquire the target; $sensor_i$ sends $sensor_{ii}$'s data to cue $sensor_{iii}$, which acquires physical connection at t_5; $sensor_{iii}$ signals to $sensor_i$ so it can maintain referential integrity while maneuvering to reacquire physical connection with the target at t_8.

Figure 4-9: Hunter leverages distributed observers to maintain reference to maneuvering target

Likewise, distributed targeting organizations construct decoupled representations by transforming and combining records of previous couplings in order to enable subsequent couplings.[847] Representations, as structured material artifacts, are themselves physically decoupled from the target environment, yet the chains of material translations running back and forth make it possible to combine together records of previous couplings (from past collection) and to enable subsequent couplings (to cue future collection). On one end the insurgent's

[847] Brian Cantwell Smith, *On the Origin of Objects* (Cambridge, MA: MIT Press, 1996), 298, observes that any cognitive system has "to connect in such a way as to support appropriate (coordinated) disconnection, and to disconnect in such a way as to support appropriately prior or subsequent connection."

activities in the world are structured, and on the other end the representations in the military organization are structured. The repeated, frequent physical interactions between the friendly and enemy structures via cascades of inscription bring these different structures into closer and closer coordination. Closer coordination progressively lowers the uncertainty of each reconnection. Intelligence collection and operational assaults alike involve these alternating episodes of connection and disconnection in order to enable reliable reconnection. Information friction complicates coordination, increases uncertainty, and frustrates reconnection.

Bibliography

Abbate, Janet. *Inventing the Internet*. Cambirdge, MA: MIT Press, 2000.

Adams, Gordon. *The Politics of Defense Contracting: the Iron Triangle*. Piscataway, NJ: Transaction Publishers, 1982.

Adams, James. *The Next World War: The Weapons and Warriors of the New Battlefields of Cyberspace*. London: Arrow, 1998.

Adams, Sam. *War of Numbers: An Intelligence Memoir*. Steerforth Press, 1998.

Adamsky, Dima P. "Through the Looking Glass: The Soviet Military-Technical Revolution and the American Revolution in Military Affairs." *Journal of Strategic Studies* vol. 31, no. 2, 2008: 257-294.

Adamsky, Dima. *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*. Stanford, CA: Stanford University Press, 2010.

Agar, Jon. *The Government Machine: A Revolutionary History of the Computer*. Cambridge, MA: MIT Press, 2003.

Agar, Michael H. *The Professional Stranger: An Informal Introduction to Ethnography, 2nd Edition*. New York, NY: Elsevier Academic Press, 1996.

Akerlof, George A. "The Market For "Lemons": Quality Uncertainty and the Market Mechanism." *The Quarterly Journal of Economics* vol. 84, no. 3, 1970: 488-500.

Alac, Morana, and Edwin Hutchins. "I See What You are Saying: Action As Cognition in FMRI Brain Mapping Practice." *Journal of Cognition and Culture* vol. 4, no. 3, 2004: 629-661.

Alberts, David S., and Richard E. Hayes. *Power to the Edge: Command...Control...in the Information Age*. Washington D.C.: CCRP Publications Series, 2003.

Alberts, David S., John J. Garstka, and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington D.C.: CCRP Publications Series, 1999.

Alberts, David S., John J. Garstka, Richard E. Hayes, and David A. Signori. *Understanding Information Age Warfare*. Washington D.C.: CCRP Publications Series, 2001.

Alexander, Matthew, and John Bruning. *How to Break a Terrorist: The U.S. Interrogators Who Used Brains, Not Brutality, to Take Down the Deadliest Man in Iraq*. New York, NY: Free Press, 2008.

Allard, Kenneth C. *Command, Control, and the Common Defense*. New Haven, CT: Yale University Press, 1990.

Alvarez, David J. *Secret Messages: Codebreaking and American Diplomacy, 1930-1945*. University Press of Kansas, 2000.

Anderson, Kenneth. "Targeted Killing in U.S. Counterterrorism Strategy and Law." *Counterterrorism and American Statutory Law Working Paper*, 11 May 2009.

Anderson, Leon. "Analytic Autoethnography." *Journal of Contemporary Ethnography* vol. 35, no. 4, 2006: 373-395.

Anderson, Ross. "Why Information Security is Hard: An Economic Perspective." *17th Annual Computer Security Applications Conference* vol. 2001, 2001: 358–365.

Andreas, Peter, and Kelly M. Greenhill (Eds.). *Sex, Drugs, and Body Counts: The Politics of Numbers in Global Crime and Conflict*. Ithaca NY: Cornell University Press, 2010.

Arendt, Hannah. *Eichmann in Jerusalem: A Report on the Banality of Evil*. New York, NY: Viking Press, 1963.

Argyres, Nicholas S. "The Impact of Information Technology on Coordination: Evidence From the B-2 "Stealth" Bomber." *Organization Science* vol. 10, no. 2, 1999: 162-180.

Arquilla, John, and David F. Ronfeldt. *In Athena's Camp: Preparing For Conflict in the Information Age*. Santa Monica, CA: RAND Corporation, 1997.

Arquilla, John, and David F. Ronfeldt. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND, 2001.

Arthur, W. Brian. "Competing Technologies, Increasing Returns, and Lock-In by Historical Events." *The Economic*

Journal vol. 99, no. 394, 1989: 116-131.

Arthur, W. Brian. *The Nature of Technology: What It Is and How It Evolves*. New York, NY: Free Press, 2009.

Atkinson, Rick. "Left of Boom: The Fight Against Roadside Bombs." *Washington Post*, September 30 2007. http://www.washingtonpost.com/wp-srv/world/specials/leftofboom/index.html.

Attewell, Paul. *Information Technology and the Productivity Paradox*. In D. Harris (Ed.), Organizational Linkages: Understanding the Productivity Paradox (Washington DC: National Academy Press): 13-53, 1994.

Aussaresses, Paul. *The Battle of the Casbah: Terrorism and Counterterrorism in Algeria 1955-1957*. New York: Enigma Books, 2002.

Avant, Deborah D. *Political Institutions and Military Change: Lessons From Peripheral Wars*. Ithaca, NY: Cornell University Press, 1994.

Bacevich, Andrew J. "Just War II: Morality and high technology." *The National Interest*, no. 45, 1996: 37-48.

Bahmanyar, Mir, and Chris Osman. *SEALs: The US Navy's Elite Fighting Force*. Oxford: Osprey Publishing, 2008.

Bahney, Benjamin, Howard J. Shatz, Carroll Ganier, Renny Mcpherson, Barbara Sude, Sara Beth Elson, and Ghassan Schbley. *An Economic Analysis of the Financial Records of Al-Qa'Ida in Iraq*. Santa Monica, CA: RAND, 2010.

Baird, Davis. *Thing Knowledge : A Philosophy of Scientific Instruments*. Berkeley: University of California Press, 2004.

Baker, Ralph O. "HUMINT-Centric Operations: Developing Actionable Intelligence in the Urban Counterinsurgency Environment." *Military Review*, March-April 2007.

Baldwin, Carliss Y., and Kim B. Clark. *Design Rules, Vol 1: The Power of Modularity*. Cambridge, MA: MIT Press, 2000.

Baldwin, Carliss, and Eric Von Hippel. "User, and Open Collaborative Innovation: Ascendant Economic Models." *Harvard Business School Finance Working Paper*, 10-038 2009.

Ball, Desmond, and Jeffrey Richelson. *Strategic Nuclear Targeting*. Ithaca, NY: Cornell University Press, 1986.

Bamford, James. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency from the Cold War Through the Dawn of a New Century*. New York, NY: Doubleday, 2001.

Bamford, James. *The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America*. New York: Anchor Books, 2008.

Barabasi, Albert-Laszlo, and Eric Bonabeau. "Scale Free Networks." *Scientific American*, May 2003.

Baram, Amatzia. "Neo-Tribalism in Iraq: Saddam Husayn's Tribal Policies 1991-1996." *Journal of Middle Eastern Studies* vol. 29, no. 1, 1997: 29-56.

Barnaby, Frank. *The Automated Battlefield*. London: Sidgwick & Jackson, Ltd, 1986.

Barnett, Jeffery R. *Defeating Insurgents With Technology*. Airpower Journal (Summer), 1996.

Baszanger, Isabella, and Nicolas Dodier. "Ethnography: Relating the Part to the Whole." In *Qualitative Research: Theory, Method and Practice*, edited by David Silverman, 9-34. London: Sage Publications, 2004.

Bateson, Gregory. *Mind and Nature*. New York: E. P. Dutton, 1979.

Bateson, Gregory. *Steps to an Ecology of Mind*. Chicago, IL: University of Chicago Press, 2000.

Bean, Hamilton. "The DNI's Open Source Center: an Organizational Communication Perspective." *International Journal of Intelligence and Counterintelligence* vol. 20, 2007: 240–257.

Becker, Markus C. "Organizational Routines: A Review of the Literature." *Industrial and Corporate Change* vol. 13, no. 4, 2004: 643-678.

Beesley, Patrick. *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Center 1939-1945*. London: Greenhill Books, 2000.

Begg, Moazzam. *Enemy Combatant: My Imprisonment At Guantanamo, Bagram, and Kandahar*. New York, NY: New Press, 2006.

Benbow, Tim. *The Magic Bullet? Understanding the Revolution in Military Affairs*. London: Brassey's, 2004.

Beniger, James R. *The Control Revolution: Technological and Economic Origins of the Information Society*.

Cambridge, MA: Harvard University Press, 1986.

Benkler, Yochai. "Coase's Penguin Or, Linux and 'The Nature of the Firm'." *The Yale Law Journal* vol. 112, no. 3, 2002: 369-446.

Benkler, Yochai. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven, CT: Yale University Press, 2007.

Betts, Richard K. "The Downside of the Cutting Edge: Disadvantages of Revolution in Military Affairs." *The National Interest*, Fall 1996.

Betts, Richard K. *Enemies of Intelligence: Knowledge and Power in American National Security*. Columbia University Press, 2007.

Betts, Richard K. *Surprise Attack: Lessons for Defense Planning*. Washington DC: Brookings Institute, 1982.

Betz, David J. "The More You Know, the Less You Understand: the Problem With Information Warfare." *The Journal of Strategic Studies* vol. 29, no. 3, 2006: 505-533.

Beyerchen, Alan. "From Radio to Radar: Interwar Military Adaptation to Technological Change in Germany, the United Kingdom, and the United States." In *Military Innovation in the Interwar Period*, edited by Williamson Murray and Allan R. Millett, 265-299. Cambridge University Press, 1996.

Biddle, Stephen D. "Allies, Airpower, and Modern Warfare: The Afghan Model in Afghanistan and Iraq." *International Security* vol. 30, no. 3, 2005: 161-176.

Biddle, Stephen. "The Past As Prologue: Assessing Theories of Future Warfare." *Security Studies* vol. 8, no. 1, 1998: 1-74.

Biddle, Stephen. *Military Power: Explaining Victory and Defeat in Modern Battle*. Princeton University Press, 2004.

Biddle, Tami Davis. *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914–1945*. Princeton, NJ: Princeton University Press, 2002.

Biggs, Michael. "Putting the State on the Map: Cartography, Territory, and European State Formation." *Comparative Studies in Society and History* vol. 41, no. 2, 1999: 374-405.

Bijker, Wiebe, Thomas P. Hughes, and Trevor Pinch (Eds.). *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA: MIT Press, 1987.

Black, Jeremy. "Military Organisations and Military Change in Historical Perspective." *The Journal of Military History* vol. 62, no. 4, 1998: 871-892.

Blackett, P. M. S. "Tizard and the Science of War." *Nature* vol. 185, no. 4714, 1960: 647–653.

Blair, Bruce G. *Strategic Command and Control: Redefining the Nuclear Threat*. Washington, DC: Brookings Institution, 1985.

Blaker, James R. *Transforming Military Force: The Legacy of Arthur Cebrowski and Network Centric Warfare*. Westport, CT: Praeger, 2007.

Borges, Jorge Luis. *Collected Fictions*. New York: Penguin, 1999.

Boslaugh, David L. *When Computers Went to Sea: The Digitization of the United States Navy*. Los Alamitos, CA: IEEE Computer Society Press, 2003.

Bourdieu, Pierre. *In Other Words: Essays Toward a Reflexive Sociology*. Stanford, CA: Stanford University Press, 1990.

Bourke, Joanna. *An Intimate History of Killing: Face-To-Face Killing in Twentieth-Century Warfare*. New York, NY: Basic Books, 1999.

Bowden, Mark. "The Ploy." *The Atlantic Monthly*, May 2007.

Bowker, Geoffrey C. "How to Be Universal: Some Cybernetic Strategies, 1943-70." *Social Studies of Science* vol. 23, no. 1, 1993: 107-127.

Bowker, Geoffrey C. *Memory Practices in the Sciences*. Cambridge, MA: MIT Press, 2006.

Bowker, Geoffrey C., and Susan Leigh Star. *Sorting Things Out: Classification and its Consequences*. Cambridge, MA: MIT Press, 1999.

Boyd, Robert, and Peter J. Richerson. *The Origin and Evolution of Cultures*. Oxford University Press, 2005.

Brachman, Jarret M. "High-Tech Terror: Al-Qaeda's Use of New Technology." *The Fletcher Forum of World Affairs* vol. 30, no. 2, 2006: 149-164.

Bracken, Paul J. *The Command and Control of Nuclear Forces*. New Haven, CT: Yale University Press, 1983.

Bracken, Paul. "Unintended Consequences of Strategic Gaming." *Simulation Gaming* vol. 8, no. 3, 1977: 283-318.

Brate, Adam (Ed.). *Technomanifestos*. New York: Texere, 2002.

Brock, Gerald W. *The Second Information Revolution*. Cambridge, MA: Harvard University Press, 2003.

Brodie, Bernard. "Technological Change, Strategic Doctrine, and Political Outcomes." In *Historical Dimensions of National Security Problems*, edited by K. Knorr, 263-306. Kansas University Press, 1976.

Brooks, Frederick P. *The Mythical Man Month: Essays on Software Engineering, 20th Anniversary Edition*. Reading, MA: Addison-Wesley Publishing Co, 1995.

Brooks, Risa, and Elizabeth A. Stanley (Eds.). *Creating Military Power: The Sources of Military Effectiveness*. Stanford, CA: Stanford University Press, 2007.

Brooks, Rodney A. *Cambrian Intelligence: The Early History of the New AI*. Cambridge, MA: MIT Press, 1999.

Brown, Ian Malcolm. *British Logistics on the Western Front: 1914-1919*. Westport, CT: Praeger, 1998.

Brynjolfsson, Erik, and Lorin M. Hitt. "Beyond Computation: Information Technology, Organizational Transformation and Business Performance." *The Journal of Economic Perspectives* vol. 14, no. 4, 2000: 23-48.

Brynjolfsson, Erik. "The Productivity Paradox of Information Technology." *Communications of the ACM* vol. 36, no. 12, 1993: 66 - 77.

Buenneke, Richard H., Jr. "Lifting the Fog of War." *Government Executive*, February 1991.

Builder, Carl. *The Masks of War: American Military Styles in Strategy and Analysis*. Baltimore, MD: Johns Hopkins University Press, 1989.

Bumiller, Elisabeth. "We Have Met the Enemy and He is Powerpoint." *New York Times*, 26 April 2010: A1.

Bungay, Stephen. *The Most Dangerous Enemy: A History of the Battle of Britain*. London: Aurum Press, 2000.

Burden, Matthew Currier. *The Blog of War: Front-Line Dispatches from Soldiers in Iraq and Afghanistan*. New York, NY: Simon and Schuster, 2006.

Butterfield, Alexander P. "The Accuracy of Intelligence Assessment: Bias, Perception, and Judgment in Analysis and Decision." *Naval War College Paper*, March 1993.

Byman, Daniel. "Do Targeted Killings Work?" *Foreign Affairs* vol. 85, no. 2, 2006: 95-111.

Campbell-Kelly, Martin. *From Airline Reservations to Sonic the Hedgehog: A History of the Software Industry*. Cambridge, MA: MIT Press, 2004.

Cancian, Mark F. "What Turned the Tide in Anbar?" *Military Review*, September-October 2009.

Carafano, James Jay. *GI Ingenuity: Improvisation , Technology, and Winning World War II*. Mechanicsburg, PA: Stackpole Books, 2006.

Carroll, Lewis, and Martin Gardner. *The Annotated Alice, The Definitive Edition*. New York, NY: WW Norton & Co, 2000.

Cebrowski, Arthur K., and John J. Garstka. "Network-Centric Warfare: Its Origin and Future." *U.S. Naval Institute Proceedings* vol. 124, no. 1, 1998.

Center of Military History. *Improvisations During the Russian Campaign*. Washington DC: United States Army, 1986.

Chandler, Alfred D., and James W. Cortada (Eds.). *A Nation Transformed By Information: How Information Has Shaped the United States From Colonial Times to the Present*. New York, NY: Oxford University Press, 2003.

Chesbrough, Henry. "Towards a Dynamics of Modularity: A Cyclical Model of Technical Advance." In *The Business of Systems Integration*, edited by Andrea Prencipe, Andrew Davies and Michael Hobday, 174-200. Oxford University Press, 2003.

Ciborra, Claudio. "Imbrication of Representations: Risk and Digital Technologies." *Journal of Management Studies*

vol. 43, no. 6, 2006: 1339–1356.

Ciborra, Claudio. *The Labyrinths of Information: Challenging the Wisdom of Systems*. New York, NY: Oxford University Press, 2002.

Clark, Andy, and David Chalmers. "The Extended Mind." *Cognitive Science* vol. 58, no. 1, 1998: 7-19.

Clark, Andy. *Supersizing the Mind: Embodiment, Action, and Cognitive Extension*. Oxford University Press, 2008.

Clark, David D. "Network Neutrality: Words of Power and 800-Pound Gorillas." *International Journal of Communication* vol. 1, 2007: 701-708.

Clark, David D., John Wroclawski, Karen R. Sollins, and Robert Braden. "Tussle in Cyberspace: Defining Tomorrow's Internet." *Ieee/acm Transactions on Networking* vol. 13, no. 3, 2005: 462-475.

Clark, David D., Karen Sollins, John Wroclawski, and Ted Faber. *Addressing Reality: an Architectural Response to Real-World Demands on the Evolving Internet*. ACM SIGCOMM 2003 Workshops, August 25&27, 2003, Karlsruhe, Germany, 2003.

Clarke, I. F. *Voices Prophesying War, 1763-1984*. New York, NY: Oxford University Press, 1966.

Clarke, Richard A., and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do about It*. New York, NY: Harpercollins, 2010.

Clausewitz, Carl von. *On War*. Trans. and ed. Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Clayton, Aileen. *The Enemy is Listening*. New York, NY: Ballentine Books, 1982.

Coakley, Thomas P. *Command and Control for War and Peace*. Washington DC: National Defense University Press, 1992.

Coase, R. H. "The Nature of the Firm." *Economica* vol. 4, no. 1, 1937: 386-405.

Coase, R. H. "The Problem of Social Cost." *Journal of Law and Economics* vol. 3, 1960: 1-44.

Cochran, Alexander S. (Ed.). *Gulf War Air Power Survey, Volume 1*. Washington, DC: Government Printing Office, 1993.

Cohen, Eliot A. "A Revolution in Warfare." *Foreign Affairs* vol. 75, no. 2, 1996: 37-54.

Cohn, Carol. "Sex and Death in the Rational World of Defense Intellectuals." *Signs* vol. 12, no. 4, 1987: 687-718.

Collins, H. M. *Artificial Experts: Social Knowledge and Intelligent Machines*. Cambridge, MA: MIT Press, 1992.

Cooling, Benjamin Franklin (Ed.). *Case Studies in the Development of Close Air Support*. Washington, DC: United States Air Force, Office of Air Force History, 1990.

Coram, Robert. *Boyd: The Fighter Pilot Who Changed the Art of War*. Boston, MA: Little, Brown and Co, 2002.

Cordesman, Anthony H. "Violence in Iraq: Reaching an 'irreducible Minimum'." *Center for Strategic and International Studies Report*, 25 February 2008. http://www.csis.org/media/csis/pubs/080227_violence.in.iraq.pdf.

Cortada, James W. *Information Technology As Business History: Issues in the History and Management of Computers*. Greenwood Press, 1996.

Cortada, James W. *The Digital Hand, Vol 3: How Computers Changed the Work of American Public Sector Industries*. New York, NY: Oxford University Press, 2008.

Cote, Owen R. "The Third Battle: Innovation in the U.S. Navy's Silent Cold War Struggle With Soviet Submarines." *Naval War College Newport Paper*, no. 16, 2003. http://www.usnwc.edu/Publications/Naval-War-College-Press/Newport-Papers/Documents/16-pdf.aspx.

Cote, Owen R. *The Politics of Innovative Military Doctrine: The US Navy and Fleet Ballistic Missiles*. Ph.D. Dissertation, MIT Department of Political Science, 1996.

Couch, Dick. *The Sheriff of Ramadi: Navy SEALs and the Winning of Anbar*. Annapolis, MD: Naval Institute Press, 2008.

Couch, Dick. *The Warrior Elite: The Forging of SEAL Class 228*. New York: Three Rivers Press, 2001.

Cowan, Ruth Schwartz. *More Work for Mother: The Ironies of Household Technology from the Open Hearth to the*

Microwave. New York, NY: Basic Books, 1983.

Cox, Sebastian. "A Comparative Analysis of RAF and Luftwaffe Intelligence in the Battle of Britain, 1940." *Intelligence and National Security* vol. 5, no. 2, 1990: 425-42.

Coyle, Diane. *The Weightless World: Strategies For Managing the Digital Economy*. Cambridge, MA: MIT Press, 1999.

Crawford, George A. *Manhunting: Counter-Network Organization for Irregular Warfare*. Joint Special Operations University Report 09-7, 2009.

Crosby, Alfred W. *The Measure of Reality: Quantification in Western Europe, 1250-1600*. Cambridge University Press, 1997.

Crosby, Alfred W. *Throwing Fire: Projectile Technology Through History*. New York, NY: Cambridge University Press, 2002.

Dao, James. "Pentagon Keeps Wary Watch As Troops Blog." *New York Times*, 9 September 2006: A1.

David, Paul A. "The Dynamo and the Computer: An Historical Perspective on the Modern Productivity Paradox." *The American Economic Review* vol. 80, no. 2, 1990: 355-361.

David, Paul A. *Understanding the Economics of QWERTY: The Necessity of History*. In W. Parker (Ed.), Economic History and the Modern Historian, pp. 30-49. London: Blackwell, 1986.

Davis, Joshua. "If We Run Out of Batteries, This War Is Screwed." *Wired*, June 2003.

Dawkins, Richard. *The Blind Watchmaker: Why the Evidence of Evolution Reveals a Universe without Design*. New York, NY: W. W. Norton & Co, 1996.

Dawood, Hosham. "The Stateization of the Tribe and the Tribalization of the State: The Case of Iraq." In *Tribes and Power: Nationalism and Ethnicity in the Middle East*, edited by Faleh Jabar and Hosham Dawood. London: Saqi Books, 2003.

Day, Dwayne A. *Eye in the Sky: The Story of the Corona Spy Satellites*. Washington, DC: Smithsonian Institute, 1999.

Defense Science Board. *Report of the Defense Science Board Task Force on Defense Software*. Washington DC (November), 2000.

Deforest, Orrin, and David Chanoff. *Slow Burn: The Rise and Bitter Fall of American Intelligence in Vietnam*. New York, NY: Simon & Schuster, 1990.

Demchak, Chris C. *Military Organizations, Complex Machines: Modernization in the U.S. Armed Services*. Ithaca, NY: Cornell University Press, 1991.

Dennett, Daniel C. *Consciousness Explained*. Boston: Little, Brown and Co., 1991.

Deptula, Dave, and Mike Francisco. "Air Force ISR Operations: Hunting Versus Gathering." *Air & Space Power Journal*, Winter 2010: 13-17.

Deutsch, Karl W. *The Nerves of Government: Models of Political Communication and Control*. New York, NY: Free Press, 1966.

Diamond, John. "Re-Examining Problems and Prospects in U.S. Imagery Intelligence." *International Journal of Intelligence and Counterintelligence* vol. 14, no. 1, 2001: 1-24.

Dickson, Paul. *The Electronic Battlefield*. Indiana University Press, 1976.

DiMaggio, Paul J., and Walter W. Powell. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality." In *The New Institutionalism in Organizational Analysis*, edited by Walter W. Powell and Paul J. DiMaggio, 63-82. Chicago, IL: University of Chicago Press, 1991.

Dombrowski, Peter J., and Eugene Gholz. *Buying Military Transformation: Technological Innovation and the Defense Industry*. New York, NY: Columbia University Press, 2006.

Doubler, Michael D. *Closing With the Enemy: How GIs Fought the War in Europe, 1944-1945*. University Press of Kansas, 1995.

Dowding, Hugh C. T. "The Battle of Britain." *Supplement to the London Gazette*, 11 Sept 1946: 4543-4571.

Downey, Greg. "Virtual Webs, Physical Technologies, and Hidden Workers: The Spaces of Labor in Information

Internetworks." *Technology and Culture* vol. 42, no. 2, 2001: 209-235.

Drea, Edward. *MacArthur's Ultra: Codebreaking and the War Against Japan: 1942-1945*. Lawrence, KS: Kansas University Press, 1992.

Drew, Christopher. "Military is Awash in Data from Drones." *New York Times*, 10 January 2010.

Dreyfus, Hubert L. *Being-in-the-World: A Commentary on Heidegger's Being and Time, Division I*. Cambridge: MIT Press, 1991.

Dreyfus, Hubert L. *What Computers Still Can't Do: A Critique of Artificial Reason*. Cambridge, MA: MIT Press, 1992.

Dreyfus, Stuart E., and Hubert L. Dreyfus. *A Five-Stage Model of the Mental Activities Involved in Directed Skill Acquisition*. University of California Operations Research Center, 1980.

Dror, Itiel E., and Stevan Harnad (Eds.). *Cognition Distributed: How Cognitive Technology Extends Our Minds*. Amsterdam: John Benjamins Publishing Co, 2008.

Dunlap, Charles J., Jr. *Technology and the 21st Century Battlefield: Recomplicating Moral Life For the Statesman and the Soldier*. Strategic Studies Institute, 1999.

Dupuy, Jean-Pierre. *The Mechanization of the Mind: On the Origins of Cognitive Science*. Princeton: Princeton University Press, 2000.

Dupuy, Trevor Nevitt. *A Genius For War: The German Army and General Staff, 1807-1945*. Englewood Cliffs, NJ: Prentice-Hall, 1977.

Eckhardt, George S. *Vietnam Studies: Command and Control 1950-1969*. Department of the Army, Center of Military History Pub 90-8, 1974.

Edwards, David B. "Counterinsurgency As a Cultural System." *Small Wars Journal*, 27 December 2010. Http://smallwarsjournal.com/blog/journal/docs-temp/630-edwards.pdf.

Edwards, Paul N. *The Closed World: Computers and the Politics of Discourse in Cold War America*. Cambridge, MA: MIT Press, 1996.

Ehlers, Robert S., Jr. *Targeting the Third Reich: Air Intelligence and the Allied Bombing Campaigns*. Lawrence, KS: Kansas University Press, 2009.

Ehrhard, Thomas P. *Unmanned Aerial Vehicles: A Comparative Study of Weapon System Innovation*. Ph.D. Dissertation, Johns Hopkins University School of Advanced International Studies, 2000.

Eichengreen, Barry. *Globalizing Capital*. Princeton University Press, 1998.

Emerson, Robert M., Rachel I. Fretz, and Linda L. Shaw. *Writing Ethnographic Fieldnotes*. Chicago, IL: University of Chicago Press, 1995.

Engelbart, Doug C. *Augmenting Human Intellect: A Conceptual Framework*. Stanford Research Institute, AFOSR-3233, 1962.

Espeland, Wendy Nelson, and Mitchell L. Stevens. "Commensuration As a Social Process." *Annual Review of Sociology* vol. 24, 1998: 313-343.

Evangelista, Matthew. "How Technology Fuels the Arms Race." *Technology Review* vol. 91, no. 5, 1988: 42-49.

Farkas, David K. "Toward a Better Understanding of Powerpoint Deck Design." *Information Design Journal + Document Design* vol. 14, no. 2, 2006: 162–171.

Farrell, Theo. "Improving in War: Military Adaptation and the British in Helmand Province, Afghanistan, 2006-2009." *Journal of Strategic Studies* vol. 33, no. 4, 2010: 567 - 594.

Feickert, Andrew. "U.S. Special Operations Forces (SOF): Background and Issues for Congress." *Congressional Research Service Report*, 16 May 2008.

Feld, M. D. "Information and Authority: The Structure of Military Organization." *American Sociological Review* vol. 24, no. 1, 1959: 15-22.

Feldman, Martha S. "A Performative Perspective on Stability and Change in Organizational Routines." *Industrial and Corporate Change* vol. 12, no. 4, 2003: 727-752.

Feldman, Martha S. *Order Without Design: Information Production and Policy Making*. Stanford University Press,

1989.

Felter, Joe, Jeff Bramlett, Bill Perkins, Jarret Brachman, Brian Fishman, James Forest, Lianne Kennedy, Jacob Shapiro, and Tom Stocking. *Harmony and Disharmony: Exploiting Al-Qa'Ida's Organizational Vulnerabilities*. West Point, NY: Center for Combating Terrorism, 2006.

Ferrell, Jeff, and Mark S. Hamm (Eds.). *Ethnography At the Edge: Crime, Deviance, and Field Research*. Boston, MA: Northeastern University Press, 1998.

Ferris, John Robert, and Michael I. Handel. "Clausewitz, Intelligence, Uncertainty and the Art of Command in Military Operations." *Intelligence and National Security* vol. 10, no. 1, 1995: 1-58.

Ferris, John Robert. "Fighter Defence Before Fighter Command: the Rise of Strategic Air Defence in Great Britain, 1917-1934." *The Journal of Military History* vol. 63, no. 4, 1999: 845-884.

Ferris, John Robert. "Netcentric Warfare, C4ISR and Information Operations: Towards a Revolution in Military Intelligence?" *Intelligence and National Security* vol. 19, no. 2, 2004: 199-225.

Ferris, John. "'Airbandit': C3I and Strategic Air Defence During the First Battle of Britain, 1915-1918." In *Strategy and Intelligence: British Policy During the First World War*, edited by Michael Dockrill and David French. London, UK: Hambledon, 1995.

Fishman, Brian (Ed.). *Bombers, Bank Accounts, and Bleedout: Al-Qaeda's Road in and Out of Iraq*. West Point, NY: Center for Combating Terrorism, 2008.

Flynn, Michael T., Rich Juergens, and Thomas L. Cantrell. "Employing ISR: SOF Best Practices." *Joint Forces Quarterly*, no. 50, 2008: 56-61.

Ford, Christopher A., and David A. Rosenberg. *The Admirals' Advantage: U.S. Navy Operational Intelligence in World War II and the Cold War*. Annapolis, MD: Naval Institute Press, 2005.

Forsythe, Diana E. "Ethics and Politics of Studying Up in Technoscience." *Anthropology of Work Review, Vol.* vol. 20, 1999: 6-11.

Forsythe, Diana E. *Studying Those Who Study Us: An Anthropologist in the World of Artificial Intelligence*. Stanford, CA: Stanford University Press, 2001.

Foucault, Michel. *Discipline and Punish: the Birth of the Prison*. New York: Vintage, 1995.

Foucault, Michel. *The Order of Things: An Archaeology of the Human Sciences*. New York: Vintage, 1994.

Friedman, George, and Meredith Friedman. *The Future of War: Power, Technology, and American World Dominance in the 21st Century*. New York, NY: Crown, 1996.

Friedman, Norman. *Seapower and Space: From the Dawn of the Missile Age to Net-Centric Warfare*. Anapolis, MD: Naval Institute Press, 2000.

Fullerton, Daryl L. "Back to the Basics: Training Army Artillerymen to Grow Afghan National Army Artillerymen." *Air Land Sea Bulletin* vol. 2008, no. 3, 2008: 4-7.

Galison, Peter Louis. *Image and Logic: A Material Culture of Microphysics*. Chicago: University of Chicago Press, 1997.

Galison, Peter. "Removing Knowledge." *Critical Inquiry* vol. 31, Autumn 2004: 229-243.

Gallie, Duncan. "Patterns of Skill Change: Upskilling, Deskilling or Polarization?" *Work, Employment & Society* vol. 5, no. 3, 1991: 319-351.

Galula, David. *Counterinsurgency Warfare: Theory and Practice*. London: Praeger Security International, 2006.

Gambetta, Diego. *Codes of the Underworld: How Criminals Communicate*. Princeton, NJ: Princeton University Press, 2009.

Ganchrow, Raviv. "Perspectives on Sound-Space: The Story of Acoustic Defense." *Leonardo Music Journal*, December 2009: 71-75.

Gates, Robert M. "Helping Others Defend Themselves." *Foreign Affairs* vol. 89, no. 3, 2010: 2-6.

Gentry, John A. "Doomed to Fail: America's Blind Faith in Military Technology." *Parameters* vol. 32, no. 4, 2002.

Georgia Institute of Technology. "Not for Pilots Only: Flight-Mapping Software Attracts Broad Audience With Its

Diverse Capabilities." *Georgia Tech Research News*, 20 June 2004.

Gerring, John. "Is There a (Viable) Crucial-Case Method?" *Comparative Political Studies* vol. 40, no. 3, 2007: 231-253.

Gerring, John. *Case Study Research: Principles and Practice*. New York, NY: Cambridge University Press, 2007.

Gholz, Eugene, Daryl G. Press, and Harvey M. Sapolsky. "Come Home, America: The Strategy of Restraint in the Face of Temptation." *International Security* vol. 21, no. 4, 1997: 5-48.

Gibson, James J. "The Theory of Affordances." In *Perceiving, Acting, and Knowing: Toward an Ecological Philosophy*, edited by Robert Shaw and John Bransford, 67-82. Hillsdale, NJ: Lawrence Erlbaum Association, 1977.

Giles, Jim. "Internet Encyclopaedias Go Head to Head." *Nature* vol. 438, 2005: 900-901.

Gill, Peter, Stephen Marrin, and Mark Pythian (Eds.). *Intelligence Theory: Key Questions and Debates*. New York, NY: Routledge, 2009.

Gillespie, Paul G. *Weapons of Choice: The Development of Precision Guided Munitions*. University Alabama Press, 2006.

Girard, René, and Benoît Chantre. *Battling to the End*. Trans. By Mary Baker. East Lansing, MI: Michigan State University, 2010.

Glaser, Barney G., and Anselm Strauss. *Discovery of Grounded Theory: Strategies For Qualitative Research*. Chicago, IL: Aldine Publishing Co, 1967.

Gleick, James. *Chaos: Making a New Science*. New York, NY: Penguin, 1987.

Goetz, Robert. *Austerlitz: Napoleon and the Destruction of the Third Coalition*. London: Greenhill, 2005.

Goldman, Emily O., and Leslie C. Eliason (Eds.). *The Diffusion of Military Technology and Ideas*. Palo Alto, CA: Stanford University Press, 2003.

Goldsmith, Jack, and Tim Wu. *Who Controls the Internet? Illusions of a Borderless World*. New York, NY: Oxford University Press, 2006.

Gompert, David C., Charles L. Barry, and Alf A. Andreassen. *Extending the User's Reach: Responsive Networking For Integrated Military Operations*. National Defense University, Center For Technology and National Security Policy, Defense and Technology Paper 24, 2006.

Gompert, David C., John Gordon, Adam Grissom, David R. Frelinger, Seth G. Jones, Martin C. Libicki, Brooke Stearns Lawson, and Robert E. Hunter. *War By Other Means: Building Complete and Balanced Capabilities for Counterinsurgency (RAND Counterinsurgency Study, Final Report)*. Santa Monica, CA: RAND Corporation, 2008.

Gordon, Michael R., and Bernard E. Trainor. *Cobra II: The Inside Story of the Invasion and Occupation of Iraq*. New York: Random House, 2006.

Gould, Stephen J. *The Structure of Evolutionary Theory*. Cambridge: Belknap Press, 2002.

Gourley, Scott R. "NAVSPECWARCOM Year in Review." *The Year in Special Operations*, 2008: 59-65.

Granovetter, Mark. "Economic Action and Social Structure: The Problem of Embeddedness." *The American Journal of Sociology* vol. 91, no. 3, 1985: 481-510.

Gray, Colin S. *Recognizing and Understanding Revolutionary Change in Warfare: The Sovereignty of Context*. Carlisle, PA: Strategic Studies Institute, 2006.

Gray, Colin S. *Weapons Don't Make War: Policy, Strategy, and Military Technology*. University Press of Kansas, 1993.

Greenhill, Kelly M. "Counting the Cost: The Politics of Numbers in Armed Conflict." In *Sex, Drugs, and Body Counts: The Politics of Numbers in Global Crime and Conflict*, edited by Peter Andreas and Kelly M. Greenhill. Ithaca NY: Cornell University Press, 2010.

Greenhill, Kelly M., and Paul Staniland. "Ten Ways to Lose At Counterinsurgency." *Civil Wars* vol. 9, no. 4, 2007: 402-419.

Grey, Christopher, and Andrew Sturdy. "A Chaos That Worked: Organizing Bletchley Park." *Public Policy and*

Administration vol. 25, no. 1, 2010: 47-66.

Grissom, Adam. "The Future of Military Innovation Studies." *The Journal of Strategic Studies* vol. 29, no. 5, 2006: 905-934.

Grossman, David. *On Killing: The Psychological Cost of Learning to Kill in War and Society*. New York, NY: Little, Brown & Co, 1995.

Gurtov, Melvin. *Viet Cong Cadres and the Cadre System: A Study of the Main and Local Forces*. Santa Monica, CA: RAND, 1967.

Guzman, Indira R., Kathryn Stam, Shaveta Hans, and Carole Angolano. "Human Factors in Security: The Role of Information Security Professionals Within Organizations." In *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions*, edited by Kenneth J. Knapp, 184-194. Hershey, NY: Information Science Reference, 2009.

Hacking, Ian. *The Social Construction of What?.* , 1999.

Hafner-Burton, Emilie M., Miles Kahler, and Alexander H. Montgomery. "Network Analysis for International Relations." *International Organization* vol. 63, no. 3, 2009: 559-592.

Halperin, Morton H. *Bureaucratic Politics and Foreign Policy*. Brookings Institution Press, 1974.

Hammes, T.X. "Dumb-Dumb Bullets: As a Decision-Making Aid, Powerpoint is a Poor Tool." *Armed Forces Journal*, July 2009.

Hanyok, Robert J. *Spartans in Darkness: American SIGINT and the Indochina War, 1945-1975*. Ft. Meade, MD: Center for Cryptologic History, 2001.

Harley, John Brian. *The New Nature of Maps: Essays in the History of Cartography*. Baltimore, MD: Johns Hopkins University Press, 2001.

Hastings, Michael. "The Runaway General." *Rolling Stone*, 1108/1109 2010. http://www.rollingstone.com/politics/news/17390/119236.

Hay, John H. *Tactical and Materiel Innovations, Vietnam Studies*. Washington, D.C.: Department of the Army, 1974.

Headrick, Daniel R. *The Invisible Weapon: Telecommunications and International Politics, 1851-1945*. Oxford University Press, 1991.

Headrick, Daniel R. *When Information Came of Age: Technologies of Knowledge in the Age of Reason and Revolution, 1700-1850*. New York, NY: Oxford University Press, 2002.

Hearn, Kelly. "Terrorist Use of Google Earth Raises Security Fears." *National Geographic News*, 12 March 2007.

Hedges, Chris. *War is a Force That Gives Us Meaning*. New York, NY: Random House, 2003.

Heide, Lars. "Monitoring People: Dynamics and Hazards of Record Management in France, 1935-1944." *Technology and Culture* vol. 45, no. 1, 2004: 80-101.

Heidegger, Martin. *Being and Time*. San Francisco, CA: Harper & Row, 1962.

Helton, J. C., and W. L. Oberkampf. "Alternative Representations of Epistemic Uncertainty." *Reliability Engineering & System Safety* vol. 85, 1-3 2004: 1-10.

Herman, Michael. *Intelligence Services in the Information Age: Theory and Practice*. London: Frank Cass, 2001.

Herrington, Stuart A. *Silence Was a Weapon: The Vietnam War in the Villages, A Personal Perspective*. Novato, CA: Presidio Press, 1982.

Hess, Charlotte, and Elinor Ostrom. "Ideas, Artifacts, and Facilities: Information As a Common-Pool Resource." *Law and Contemporary Problems* vol. 66, 1/2 2003: 111-145.

Hess, Charlotte, and Elinor Ostrom. *Understanding Knowledge As a Commons: From Theory to Practice*. Cambridge, MA: MIT Press, 2007.

Heuer, Richards J., Jr. *Psychology of Intelligence Analysis*. Washington, DC: Center For the Study of Intelligence, 1999.

Hillman, James. *A Terrible Love of War*. New York, NY: Penguin Books, 2004.

Hittle, James. D. *The Military Staff: Its History and Development*. Harrisburg, PA: Stackpole Company, 1961.

Hitz, Frederick Porter. *The Great Game: The Myths and Reality of Espionage*. New York, NY: Vintage, 2004.

Hoffman, Bruce. "The Use of the Internet By Islamic Extremists." *Testimony to the House Permanent Select Committee on Intelligence*, 4 May 2006.

Hoffman, Frank G. "Complex Irregular Warfare: the Next Revolution in Military Affairs." *Orbis* vol. 50, no. 3, 2006: 395-411.

Hollan, James, Edwin Hutchins, and David Kirsh. "Distributed Cognition: Toward a New Foundation For Human-Computer Interaction Research." *ACM Transactions on Computer-Human Interaction* vol. 7, no. 2, 2000: 174-196.

Holland, John Henry. *Emergence: From Chaos to Order*. Reading, MA: Addison-Wesley, 1998.

Holley, Irving Brinton. *Ideas and Weapons*. New Haven, CT: Yale University Press, 1953.

Holman, Brett. "The Widening Margin." *Airminded Blog*, 27 May 2008. Http://airminded.org/2008/05/27/the-widening-margin/.

Hoskin, Keith W., and Richard H. Macve. "The Genesis of Accountability: The West Point Connections." *Accounting, Organizations and Society* vol. 13, no. 1, 1988: 37-73.

Hosmer, Stephen T., and Sibylle O. Crane. *Counterinsurgency: A Symposium, April 16-20, 1962*. Santa Monica, CA: RAND Corporation, 1962. http://www.rand.org/pubs/reports/2006/R412-1.pdf.

Hughes, J. (Ed.). *Moltke on the Art of War: Selected Writings*. Novato, CA: Presidio Press, 1993.

Hughes, Thomas P. *Human-Built World: How to Think about Technology and Culture*. Chicago, IL: Univesity of Chicago Press, 2004.

Hughes, Thomas P. *Networks of Power: Electrification in Western Society, 1880-1930*. Baltimore MD: Johns Hopkins Press, 1983.

Hughes, Thomas P. *Rescuing Prometheus: Four Monumental Projects That Changed the Modern World*. New York, NY: Vintage, 1998.

Hugill, Peter J. *Global Communications Since 1844: Geopolitics and Technology*. Baltimore, MD: Johns Hopkins University Press, 1999.

Hutchby, Ian. "Technologies, Texts and Affordances." *Sociology* vol. 35, no. 2, 2001: 441-456.

Hutchins, Edwin. "How a Cockpit Remembers Its Speeds." *Cognitive Science* vol. 19, no. 3, 1995: 265-288.

Hutchins, Edwin. *Cognition in the Wild*. Cambridge, MA: MIT Press, 1995.

Ihde, Don. *Technology and the Lifeworld: From Garden to Earth*. Bloomington, IN: Indiana University Press, 1990.

Innis, Harold A. *The Bias of Communication*. Toronto: University of Toronto, 1951.

Innocenti, Charles W., Ted L. Martens, and Daniel E. Soller. "Direct Support HUMINT in Operation Iraqi Freedom." *Military Review*, May-June 2009: 48-56.

Intelligence Science Board. *Educing Information: Interrogation: Science and Art*. Washington, DC: National Defense Intelligence College Press, 2006.

Irvine, Dallas D. "The Origin of Capital Staffs." *The Journal of Modern History* vol. 10, no. 2, 1938: 161-179.

Jackson, Colin F. "Fighting for Feudalism? Dilemmas of State Consolidation in Iraq and Afghanistan." *Paper presented at International Studies Association Annual Convention, New York*, February 2009.

Jackson, Colin F. *Defeat in Victory: Organizational Learning Dysfunction in Counterinsurgency*. Ph.D. Dissertation, Massachusetts Institute of Technology, 2008.

Jaffe, Greg. "What's Your Point Lieutenant, Please? Just Cut to the Pie Charts." *Wall Street Journal*, 26 April 2000: 1.

James, William. *Principles of Psychology*. New York, NY: Henry Holt & Co, 1890.

Janowitz, Morris. "Changing Patterns of Organizational Authority: The Military Establishment." *Administrative Science Quarterly* vol. 3, no. 4, 1959: 473-493.

Janowitz, Morris. *Sociology and the Military Establishment, Revised Edition*. New York, NY: Russell Sage Foundation, 1965.

Janowitz, Morris. *The Professional Soldier: A Social and Political Portrait*. New York, NY: Free Press, 1960.

Jasanoff, Sheila. "Contested Boundaries in Policy-Relevant Science." *Social Studies of Science* vol. 17, no. 2, 1987: 195-230.

Jervis, Robert. *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon*. Ithaca, NY: Cornell University Press, 1989.

Jervis, Robert. *Perception and Misperception in International Politics*. Princeton, NJ: Princeton University Press, 1976.

Jervis, Robert. *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War*. Ithaca NY: Cornell University Press, 2010.

Jimenez, Marianela. "OAS Urges Talks in Central America Google Map Spat." *Washington Post*, November 9 2010.

Joes, Anthony James. *Resisting Rebellion: The History and Politics of Counterinsurgency*. University Press of Kentucky, 2006.

Johnson, Kenneth T. "Developments in Air Targeting: Progress and Future." *Studies in Intelligence* vol. 3, no. 3, 1959: 53-62.

Jomini, Baron Henri de. *The Art of War*. Trans. By G.H. Mendell and W.P. Craighill, Project Gutenberg Ebook, 2004.

Jones, Derek. "Understanding the Form, Function, and Logic of Clandestine Cellular Networks: The First Step in Effective Counternetwork Operations." *USACGSC School of Advanced Military Studies Paper*, 2009.

Jones, Seth G., and Martin C. Libicki. *How Terrorist Groups End Lessons for Countering Al Qa'Ida*. Santa Monica, CA: RAND Corporation, 2008.

Jones, Wilbur D. *Arming the Eagle: A History of United States Weapons Acquisition Since 1775*. Fort Belvoir, VA: Defense Systems Management College Press, 1999.

Jordan, Jenna. "When Heads Roll: Assessing the Effectiveness of Leadership Decapitation." *Security Studies* vol. 18, no. 4, 2009: 719–755.

Jorgenson, Dale W., Kevin J. Stiroh, Robert J. Gordon, and Daniel E. Sichel. "Raising the Speed Limit: U.S. Economic Growth in the Information Age." *Brookings Papers on Economic Activity* vol. 2000, no. 1, 2000: 125-235.

Kagan, Frederick. *Finding the Target: the Transformation of American Military Policy*. New York, NY: Encounter Books, 2006.

Kahn, David. "An Historical Theory of Intelligence." *Intelligence and National Security* vol. 16, no. 3, 2001: 79-92.

Kahn, David. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet, Rev. Ed.*. New York, NY: Scribner, 1996.

Kalathil, Shanthi, and Taylor C. Boas. *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*. Washington DC: Carnegie Endowment for International Peace, 2003.

Kalyvas, Stathis N. "Review: The New U.S. Army/Marine Corps Counterinsurgency Field Manual." *Perspectives on Politics* vol. 6, no. 2, 2008: 351-353.

Kalyvas, Stathis N. *The Logic of Violence in Civil War*. Cambridge University Press, 2006.

Kauffman, Stuart A. *The Origins of Order: Self-Organization and Selection in Evolution*. New York, NY: Oxford University Press, 1993.

Kaufman, Herbert. *Are Government Organizations Immortal?*. Washington DC: Brookings Institution, 1976.

Keegan, John. *The Second World War*. New York, NY: Viking, 1990.

Kelly, Thomas L., and John P. Andreasen. "Joint Fires A BCD Perspective in Operation Iraqi Freedom." *Field Artillery*, November-December 2003: 20-25.

Kier, Elizabeth. *Imagining War: French and British Military Doctrine Between the Wars*. Princeton, NJ: Princeton University Press, 1999.

Kipp, Jacob, Lester Grau, Karl Prinslow, and Don Smith. "The Human Terrain System: A CORDS For the 21st Century." *Military Review*, September-October 2006.

Kirby, M., and R. Capey. "The Air Defence of Great Britain, 1920-1940: An Operational Research Perspective."

Journal of the Operational Research Society vol. 48, no. 6, 1997: 555-568.

Kirby, M., and R. Capey. "The Area Bombing of Germany in World War II: An Operational Research Perspective." *The Journal of the Operational Research Society* vol. 48, no. 7, 1997: 661-677.

Kirsh, David, and Paul Maglio. "On Distinguishing Epistemic From Pragmatic Action." *Cognitive Science* vol. 18, no. 4, 1994: 513-549.

Kitson, Frank. *Low Intensity Operations: Subversion, Insurgency, Peace-Keeping*. Harrisburg, PA: Stackpole Books, 1971.

Kline, Ronald, and Trevor Pinch. "Users As Agents of Technological Change: the Social Construction of the Automobile in the Rural United States." *Technology and Culture* vol. 37, no. 4, 1996: 763-795.

Knox, Macgregor, and Williamson Murray (Eds.). *The Dynamics of Military Revolution, 1300-2050*. Cambridge University Press, 2001.

Kometer, Michael W. *Command in Air War: Centralized Versus Decentralized Control of Combat Airpower*. Maxwell Air Force Base, AL: Air University Press, 2007.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. *Cyberpower and National Security*. Washington DC: National Defense University Press, 2009.

Kraska, Peter. B. "Enjoying Militarism: Political/personal Dilemmas in Studying U.S. Police Paramilitary Units." In *Ethnography At the Edge: Crime, Deviance, and Field Research*, edited by Jeff Ferrell and Mark S. Hamm, 88-110. Boston, MA: Northeastern University Press, 1998.

Krause, Peter John Paul. "The Last Good Chance: A Reassessment of U.S. Operations At Tora Bora." *Operations At Tora Bora. Security Studies* vol. 17, no. 4, 2008: 644 - 684.

Krepinevich, Andrew F., Jr. "Cavalry to Computer: The Pattern of Military Revolutions." *National Interest* vol. 37, 1994: 30-42.

Krepinevich, Andrew F., Jr. *The Military-Technical Revolution: A Preliminary Assessment*. Washington, DC: Center For Strategic and Budgetary Assessments, 2002.

Lagouranis, Tony, and Allen Mikaelian. *Fear Up Harsh: An Army Interrogator's Dark Journey Through Iraq*. New York, NY: Penguin Books, 2007.

Lampland, Martha, and Susan Leigh Star. *Standards and Their Stories: How Quantifying, Classifying, and Formalizing Practices Shape Everyday Life*. Ithaca NY: Cornell University Press, 2009.

Landauer, Thomas K. *The Trouble With Computers: Usefulness, Usability, and Productivity*. Cambridge, MA: MIT Press, 1996.

Latour, Bruno. "Drawing Things Together." In *Scientific Practice and Ordinary Action: Ethnomethodology and Social Studies of Science*, edited by Michael Lynch, 19-68. Cambridge University Press, 1990.

Latour, Bruno. *Pandora's Hope: Essays on the Reality of Science Studies*. Cambridge, MA: Harvard University Press, 1999.

Latour, Bruno. *Science in Action: How to Follow Scientists and Engineers Through Society*. Cambridge, MA: Harvard University Press, 1988.

Law, John. "Technology and Heterogeneous Engineering: The Case of Portuguese Expansion." In *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*, edited by Wiebe Bijker, Thomas P. Hughes and Trevor Pinch, 111-134. Cambridge, MA: MIT Press, 1987.

Lawson, Joel Jr. "Command Control as a Process." *IEEE Control Systems Magazine* vol. 1, no. 1, 1981: 5- 11.

Lehr, Bill, and Frank Lichtenberg. "Information Technology and Its Impact on Productivity: Firm-Level Evidence From Government and Private Data Sources, 1977-1993." *The Canadian Journal of Economics* vol. 32, no. 2, 1999: 335-362.

Lerner, Josh, and Jean Tirole. "Some Simple Economics of Open Source." *The Journal of Industrial Economics* vol. 50, no. 2, 2002: 197-234.

Lessig, Lawrence. "The New Chicago School." *Journal of Legal Studies* vol. 27, no. 2, 1998: 661-691.

Lessig, Lawrence. *The Future of Ideas: The Fate of the Commons in a Connected World*. New York, NY: Random

House, 2001.

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press, 2007.

Libicki, Martin C., David C. Gompert, David R. Frelinger, and Raymond Smith. *Byting Back: Regaining Information Superiority Against 21st-Century Insurgents, RAND Counterinsurgency Study, Volume 1*. Santa Monica, CA: RAND Corporation, 2007.

Licklider, J. C. R. "Man-Computer Symbiosis." *IRE Transactions on Human Factors in Electronics* vol. 1, March 1960: 4-11.

Lieber, Keir A. "The New History of World War I and What It Means For International Relations Theory." *International Security* vol. 32, no. 2, 2007: 155-191.

Lieber, Keir A. *War and the Engineers: The Primacy of Politics Over Technology*. Ithaca, NY: Cornell University Press, 2005.

Liebowitz, Ruth. *Acquiring the Air and Space Operations Center: The AOC WS System Program Office, a Short History 2000-2003*. Hanscom Air Force Base, MA: Air Force Electronic Systems Center, 2006.

Liebowitz, S. J., and Stephen E. Margolis. "The Fable of the Keys." *Journal of Law and Economics* vol. 33, no. 1, 1990: 1-25.

Light, Jennifer S. "When Computers Were Women." *Technology and Culture* vol. 40, no. 3, 1999: 455-83.

Light, Paul C. "The New True Size of Government." *Organizational Performance Initiative, Research Brief*, no. 2, 2006. http://wagner.nyu.edu/performance/files/True_Size.pdf.

Liker, Jeffrey K., Carol J. Haddad, and Jennifer Karlin. "Perspectives on Technology and Work Organization." *Annual Review of Sociology* vol. 25, 1999: 575-5–96.

Lindsay, Jon R. "War upon the Map: User Innovation in American Military Software." *Technology and Culture* vol. 51, no. 3, 2010: 619-651.

Lindsay, Jon. "Does the 'surge' Explain Iraq's Improved Security?" *MIT Center for International Studies, Audit of the Conventional Wisdom*, September 2008.

Linzer, Dafna, and Thomas E. Ricks. "Marines' Outlook in Iraq: Anbar Picture Grows Clearer, and Bleaker." *Washington Post*, 28 November 2006: A1.

Lipsky, Michael. *Street-Level Bureaucracy: Dilemmas of the Individual in Public Services*. New York: Russell Sage Foundation, 1980.

Long, Austin, and Colin F. Jackson. "The Fifth Service: The Rise of Special Operations Command." In *US Military Innovation After the Cold War: Creation Without Destruction*, edited by Harvey M. Sapolsky, Benjamin H. Friedman and Brendan Rittenhouse Green. New York, NY: Routledge, 2009.

Long, Austin. "Small is Beautiful: The Counterterrorism Option in Afghanistan." *Orbis* vol. 54, no. 2, 2010.

Long, Austin. "The Anbar Awakening." *Survival* vol. 50, no. 2, 2008: 67-94.

Long, Austin. *First War Syndrome: Military Culture, Professionalization, and Counterinsurgency Doctrine*. Ph.D. Dissertation, Massachusetts Institute of Technology, 2010.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. Washington DC: CQPress, 2000.

Lubold, Gordon. "As Drones Multiply in Iraq and Afghanistan, So Do Their Uses." *Christian Science Monitor*, 2 March 2010.

Luck, Gary, and Mike Findlay. "Special Operations and Conventional Force Integration." *United States Joint Forces Command, Joint Warfighting Center, Focus Paper*, no. 5, 2008.

Lucsko, David N. *The Business of Speed: The Hot Rod Industry in America, 1915-1990*. Baltimore, MD: The Johns Hopkins University Press, 2008.

Ludvigsen, Eric C. "Lifting the Fog of War." *Army*, July 1972: 31.

Luttwak, Edward N. "The Operational Level of War." *International Security* vol. 5, no. 3, 1981: 61-79.

Lynn, John A. (Ed.). *Tools of War: Instruments, Ideas, and Institutions of Warfare, 1445-1871*. University of Illinois

Press, 1990.

Mackenzie, Donald A. *Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance*. Cambridge, MA: MIT Press, 1993.

MacKenzie, Donald. "The Credit Crisis As a Problem in the Sociology of Knowledge." *Unpublished Working Paper*, September 2010. http://www.sps.ed.ac.uk/__data/assets/pdf_file/0019/36082/CrisisRevised.pdf.

MacKenzie, Donald. *An Engine, Not a Camera: How Financial Models Shape Markets*. Cambridge, MA: MIT Press, 2006.

Mackey, Chris, and Greg Miller. *The Interrogators: Inside the Secret War Against Al-Qaeda*. New York, NY: Little, Brown and Company, 2004.

Macleod, Scott, and Bill Powell. "Zarqawi's Last Dinner Party." *Time*, 11 June 2006.

Mahnken, Thomas G. *Technology and the American Way of War Since 1945*. New York, NY: Columbia University Press, 2008.

Mallett, Robert L. "Why Standards Matter." *Issues in Science and Technology Online*, Winter 1998. http://www.issues.org/15.2/mallett.htm.

Mandel, Robert. "The Wartime Utility of Precision Versus Brute Force in Weaponry." *Armed Forces & Society* vol. 30, no. 2, 2004: 171-201.

Manning, Peter K., and John Van Maanen (Eds.). *Policing: A View From the Street*. New York, NY: Random House, 1978.

March, James G., and Herbert A. Simon. *Organizations, 2nd Edition*. Blackwell Publishers, 1993.

Marks, Steven M., Thomas M. Meer, and Matthew T. Nilson. "Manhunting: A Methodology for Finding Persons of National Interest." *Naval Post Graduate School, Masters Thesis*, June 2005.

Markus, Lynne M. "Electronic Mail As the Medium of Managerial Choice." *Organization Science* vol. 5, no. 4, 1994: 502-527.

Marquis, Susan L. *Unconventional Warfare: Rebuilding U.S. Special Operations Forces*. Brookings Institution Press, 1997.

Mason, Tony. *Air Power: A Centennial Appraisal*. London, Brassy's, 1994.

Mattis, James N. "USJFCOM Commander's Guidance For Effects-Based Operations." *Joint Forces Quarterly*, no. 51, 2008: 105-108.

Mauthner, N. S., and A. Doucet. "Reflexive Accounts and Accounts of Reflexivity in Qualitative Data Analysis." *Sociology* vol. 37, no. 3, 2003: 413-432.

McCary, John A. "The Anbar Awakening: an Alliance of Incentives." *The Washington Quarterly* vol. 32, no. 1, 2009: 43-59.

McCray, Lawrence E., Kenneth A. Oye, and Arthur C. Petersen. "Planned Adaptation in Risk Regulation: An Initial Survey of US Environmental, Health, and Safety Regulation." *Technological Forecasting and Social Change* vol. 77, no. 6, 2010: 951-959.

McDermott, John J. (Ed.). *The Writings of William James: A Comprehensive Edition*. Chicago, IL: University of Chicago Press, 1977.

McFarland, Stephen L. *America's Pursuit of Precision Bombing 1910-1945*. Washington, DC: Smithsonian Institute, 1995.

McGrath, John J. "The Other End of the Spear: The Tooth-to-Tail Ratio (T3R) in Modern Military Operations." *The Long War Series Occasional Paper 23, Fort Leavenworth, Kansas*, 2007.

McKeown, Timothy J. "Case Studies and the Statistical Worldview: Review of King, Keohane, and Verba's Designing Social Inquiry: Scientific Inference in Qualitative Research." *International Organization* vol. 53, no. 1, 1999: 161-190.

McMaster, H.R. "Crack in the Foundation: Defense Transformation and the Underlying Assumption of Dominant Knowledge in Future War." *US Army War College Center For Strategic Leadership, Student Issue Paper*, S03-

03 2003.

McNaugher, Thomas L. "Weapons Procurement: The Futility of Reform." In *America's Defense*, edited by Michael Mandelbaum, 68-112. New York, NY: Holmes & Meier Publishers, 1989.

McNeill, William G. *The Pursuit of Power: Technology, Armed Force, and Society Since A.D. 1000*. University of Chicago Press, 1982.

McRaven, William H. *Spec Ops: Case Studies in Special Operations Warfare Theory and Practice*. Novato, CA: Presidio Press, 1995.

Meilinger, Phillip S. "A History of Effects-Based Air Operations." *Journal of Military History* vol. 71, no. 1, 2006: 139-167.

Merleau-Ponty, Maurice. *Phenomenology of Perception*. New York: Routledge, 2002.

Messerschmitt, David G., and Clemens Szyperski. *Software Ecosystem: Understanding an Indispensable Technology and Industry*. Cambridge, MA: MIT Press, 2003.

Milgrom, Paul, and John Roberts. "An Economic Approach to Influence Activities in Organizations." *American Journal of Sociology* vol. 94, 1988: S154-S179.

Millett, Allan R., and Williamson Murray. *Military Effectiveness: The First World War*. New York: Routledge, 1991.

Millett, Allan R., Williamson Murray, and Kenneth H. Watman. "The Effectiveness of Military Organizations." *International Security* vol. 11, no. 1, 1986: 37-71.

Mindell, David A. "Automation's Finest Hour Radar and System Integration in World War II." In *Systems, Experts, and Computers: the Systems Approach in Management and Engineering, World War II and After*, edited by Agatha C. Hughes and Thomas P. Hughes, 27-56. The MIT Press, 2000.

Mindell, David A. *Between Human and Machine: Feedback, Control, and Computing Before Cybernetics*. Baltimore, MD: Johns Hopkins University Press, 2002.

Moe, Terry M. "Political Institutions: The Neglected Side of the Story." *Journal of Law, Economics, & Organization* vol. 6, special Issue 1990: 213-253.

Molnar, Andrew R., Jerry M. Tinker, and John D. Lenoir. *Human Factors Considerations of Undergrounds in Insurgencies*. Washington DC: Special Operations Research Office, The American University, 1972.

Morehouse, Jim. "Time Critical Targeting." *Presentation at National Defense Industrial Association DoD Interoperability Conference*, 26 March 2002. http://www.dtic.mil/ndia/2002interop/morehouse.pdf.

Morselli, Carlo. *Inside Criminal Networks*. New York, NY: Springer, 2009.

Mosco, Vincent. *The Digital Sublime: Myth, Power, and Cyberspace*. Cambridge, MA: MIT Press, 2004.

Moskos, Peter. *Cop in the Hood: My Year Policing Baltimore's Eastern District*. Princeton, NJ: Princeton University Press, 2008.

Moynihan, Daniel P. *Secrecy: The American Experience*. New Haven, CT: Yale University Press, 1988.

Mulvenon, James. "PLA Computer Network Operations: Scenarios, Doctrine, Organiations, and Capability." In *Beyond the Strait: PLA Missions Other Than Taiwan*, edited by Roy Kamphausen, David Lai and Andrew Scobell, 253-286. U.S. Army War College Strategic Studies Institute, 2009.

Murray, Williamson, and Allan R. Millett (Eds.). *Military Innovation in the Interwar Period*. Cambridge University Press, 1996.

Murray, Williamson. *British and German Air Doctrine Between the Wars*. Air University Review (March-April), 1980.

Myers, Steven Lee. "Chinese Embassy Bombing: A Wide Net of Blame." *New York Times*, 17 April 2000.

Nader, Laura. "Up the Anthropologist: Perspectives Gained from Studying Up." In *Reinventing Anthropology*, edited by Dell H. Hymes, 284-311. New York, Pantheon Books, 1972.

Naylor, Sean D. "More Than Door-Kickers." *Armed Forces Journal*, March 2006.

Naylor, Sean D. "Petraeus Sounds Off on Afghanistan: General Says Killing or Capturing Bin Laden Not Enough in Battle Against Al-Qaida." *Army Times*, 21 Oct 2008.

Naylor, Sean D. "Success Against Enemy Not Measured in Kills, Says Terrorism Official." *Army Times*, 4 December

2006.

Naylor, Sean D. "Support Grows for Standing Up an Unconventional Warfare Command." *Armed Forces Journal*, September 2007.

Naylor, Sean D. *Not a Good Day to Die: The Untold Story of Operation Anaconda*. New York, NY: Berkley Books, 2005.

Neale, B. T. "CH: The First Operational Radar." *GEC Journal of Research* vol. 3, no. 2, 1985: 73-83.

Negroponte, Nicholas. *Being digital*. New York, NY: Knopf, 1995.

Nelson, Richard R., and Sidney G. Winter. *Evolutionary Theory of Economic Change*. Cambridge, MA: Belknap Press, 1982.

Newmyer, Jacqueline. "The Revolution in Military Affairs With Chinese Characteristics." *Journal of Strategic Studies* vol. 33, no. 4, 2010: 483 – 504.

Nickles, David Paull. *Under the Wire: How the Telegraph Changed Diplomacy*. Harvard University Press, 2003.

Noble, David F. *Forces of Production: A Social History of Industrial Automation*. New York, NY: Knopf, 1984.

Noë, Alva. *Action in Perception*. Cambridge, MA: MIT Press, 2004.

Noë, Alva. *Out of Our Heads: Why You Are Not Your Brain, and Other Lessons from the Biology of Consciousness*. New York: Farrar, Straus, and Giroux, 2009.

Nordstrom, Carolyn, and Antonius C.G.M. Robbins. *Fieldwork under Fire*. University of California Press, 1995.

Norman, Donald A. "Affordance, Conventions, and Design." *Interactions, ACM*, May/June 1999.

Norman, Donald A. *The Design of Everyday Things*. New York, NY: Basic Books, 1988.

North, Douglass C. "Institutions." *The Journal of Economic Perspectives* vol. 5, no. 1, 1991: 97-112.

North, Douglass C. *Institutions, Institutional Change, and Economic Performance*. Cambridge University Press, 1990.

Nye, David E. *American Technological Sublime*. Cambridge, MA: MIT Press, 1996.

Nye, David E. *Technology Matters: Questions to Live With*. Cambridge, MA: MIT Press, 2006.

O'hanlon, Michael E., and Jason H. Campbell. "Iraq Index: Tracking Variables of Reconstruction & Security in Post-Saddamiraq." *Brookings Institution Report*, 28 May 2009. http://www.brookings.edu/iraqindex.

Obstfeld, Maurice, Jay C. Shambaugh, and Alan M. Taylor. "The Trilemma in History: Tradeoffs Among Exchange Rates, Monetary Policies, and Capital Mobility." *Review of Economics and Statistics* vol. 87, no. 3, 2005: 423-438.

Odierno, Raymond T., Nichoel E. Brooks, and Francesco P. Mastracchio. "ISR Evolution in the Iraqi Theater." *Joint Forces Quarterly*, no. 50, 2008: 51-55.

Odling-Smee, F. John, Kevin N. Laland, and Marcus W. Feldman. *Niche Construction: The Neglected Process in Evolution*. Princeton, NJ: Princeton University Press, 2003.

Oettinger, Anthony G. "Telling Ripe from Hype in Multimedia: The Ecstacy and the Agony." In *The Information Resources Policy Handbook: Research For the Information Age*, edited by Benjamin M. Compaine and William H. Read, 3-28. Cambridge, MA: MIT Press, 1999.

Oettinger, Anthony G. *Compunications in the National Decision-Making Process*. In Martin Greenberger (Ed.), Computers, Communications and the Public Interest. Baltimore MD: Johns Hopkins University Press: 73-114, 1971.

Office of Technology Assessment. "New Technology For NATO: Implementing Follow-On Force Attack." *U.S. Congress, OTA-ISC-309*, June 1987.

O'Hanlon, Michael E. *Technological Change and the Future of Warfare*. Washington DC: Brookings Institution Press, 2000.

Olson, Mancur. *The Logic of Collective Action: Public Goods and the Theory of Groups, 2nd Ed.*. Cambridge, MA: Harvard University Press, 1971.

Oppel, Richard A., Jr., Mark Mazzetti, and Souad Mekhennet. "Attacker in Afghanistan Was a Double Agent." *New*

York Times, 4 January 2010.

Orlikowski, Wanda J. "Improvising Organizational Transformation Over Time: A Situated Change Perspective." *Information Systems Research* vol. 7, no. 1, 1996: 63-93.

Orlikowski, Wanda J. "The Duality of Technology: Rethinking the Concept of Technology in Organizations." *Organization Science* vol. 3, no. 3, 1992: 398-427.

Orlikowski, Wanda J. "Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations." *Organization Science* vol. 11, no. 4, 2000: 404-428.

Orlikowski, Wanda J., and C. Suzanne Iacono. *The Truth Is Not Out There: an Enacted View of the "Digital Economy"*. In Erik Brynjolfsson and Brian Kahin (Eds.), Understanding the Digital Economy: Data, Tools, and Research (Cambridge, MA: MIT Press), Pp. 352-80, 2000.

Ostrom, Elinor. *Governing the Commons: The Evolution of Institutions for Collective Action*. New York, NY: Cambridge University Press, 1990.

Oudshoorn, Nelly, and Trevor Pinch (Eds.). *How Users Matter: the Co-Construction of Users and Technology*. Cambridge MA: MIT Press, 2003.

Overy, Richard J. *The Battle of Britain: The Myth and the Reality*. New York, NY: W. W. Norton, 2000.

Owens, William A. "The Emerging U.S. System-of-Systems." *National Defense University Strategic Forum* vol. 63, 1996.

Owens, William A., and Edward Offley. *Lifting the Fog of War*. New York, NY: Farrar, Straus and Giroux, 2000.

Oye, Kenneth A. (Ed.). *Cooperation Under Anarchy*. Princeton, NJ: Princeton University Press, 1986.

Palmer, Michael A. ""The Soul's Right Hand" Command and Control in the Age of Fighting Sail: 1652-1827." *The Journal of Military History* vol. 61, no. 4, 1997: 679-705.

Pape, Robert A. *Bombing to Win: Air Power and Coercion in War*. Ithaca, NY: Cornell University Press, 1996.

Paret, Peter. "Clausewitz." In *Makers of Modern Strategy: From Machiavelli to the Nuclear Age*, edited by Peter Paret. Princeton, NJ: Princeton University Press, 1986.

Paret, Peter. "The Genesis of *On War*." Preface to *On War* by Carl von Clausewitz. Princeton, NJ: Princeton University Press, 1976.

Paret, Peter. *Clausewitz and the State*. Princeton, NJ: Princeton University Press, 1985.

Pearson, David E. *The World Wide Military Command and Control System: Evolution and Effectiveness*. Maxwell Air Force Base, AL: Air University Press, 2000.

Pentland, Brian T., and Martha S. Feldman. "Organizational Routines As a Unit of Analysis." *Industrial and Corporate Change* vol. 14, 2005: 793-815.

Perrow, Charles. *Normal Accidents: Living with High Risk Technologies*. Princeton, NJ: Princeton University Press, 1999.

Perry, William G. "Information Warfare: Assuring Digital Intelligence Collection." *Joint Special Operations University Report*, 09-1 2009.

Petersen, Roger D. *Resistance and Rebellion: Lessons From Eastern Europe*. New York, NY: Cambridge University Press, 2001.

Peuquet, Donna J., and Todd Bacastow. "Organizational Issues in the Development of Geographical Information Systems: A Case Study of U.S. Army Topographic Information Automation." *International Journal of Geographical Information Science* vol. 5, no. 3, 1991: 303 - 319.

Pickering, Andrew. *The Mangle of Practice: Time, Agency, and Science*. University of Chicago Press, 1995.

Pierson, Paul. "Increasing Returns, Path Dependence, and the Study of Politics." *The American Political Science Review* vol. 94, no. 2, 2000: 251-267.

Pollack, Kenneth M. *Arabs At War: Military Effectiveness, 1948-1991*. University of Nebraska Press, 2004.

Pool, Ithiel De Sola. *Technologies of Freedom: On Free Speech in an Electronic Age*. Cambridge, MA: Belknap Press, 1983.

Posen, Barry R. "Command of the Commons: The Military Foundation of U.S. Hegemony." *International Security* vol. 28, no. 1, 2003: 5-46.

Posen, Barry R. "Is NATO Decisively Outnumbered?" *International Security* vol. 12, no. 4, 1988: 186-202.

Posen, Barry R. *Inadvertent Escalation: Conventional War and Nuclear Risks*. Cornell University Press, 1992.

Posen, Barry R. *Sources of Military Doctrine: France, Britain and Germany Between the World Wars*. Ithaca, NY: Cornell University Press, 1984.

Posen, Barry R., and Andrew L. Ross. "Competing Visions for U.S. Grand Strategy." *International Security* vol. 21, no. 3, 1997: 5-53.

Powell, Walter W. "Neither Market Nor Hierarchy: Network Forms of Organization." *Research in Organizational Behavior* vol. 12, 1990: 295-336.

Powell, Walter W., and Kaisa Snellman. "The Knowledge Economy." *Annual Review of Sociology* vol. 30, 2004: 199-220.

Prados, John. *Presidents' Secret Wars: CIA and Pentagon Covert Operations since World War II*. New York, NY: W. Morrow, 1986.

Prencipe, Andrea, Andrew Davies, and Michael Hobday (Eds.). *The Business of Systems Integration*. Oxford University Press, 2003.

Price, Alfred. *The History of US Electronic Warfare*. Arlington, VA: Association of Old Crows, 1984.

Priest, Dana, and William M. Arkin. "National Security Inc." *Washington Post*, 20 July 2010.

Prikhodko, I. E. *Characteristics of Agent Communications and of Agent Handling in the United States of America*. San Francisco, CA: Interservice Publishing, 1981.

Pritchard, David. *The Radar War: Germany's Pioneering Achievement 1904-45*. Wellingborough, U.K.: Patrick Stephens Ltd, 1989.

Probert, Henry, and Sebastian Cox. *The Battle Re-Thought: A Symposium on the Battle of Britain*. Shrewsbury, U.K.: Airlife Publishing Ltd., 1990.

Quine, W.V.O. *Word and Object*. Cambridge, MA: The MIT Press, 1960.

Rattray, Gregory J. *Strategic Warfare in Cyberspace*. Cambridge, MA: MIT Press, 2001.

Ray, John. *The Battle of Britain, New Perspectives: Behind the Scenes of the Great Air War*. London, U.K.: Arms and Armour, 1994.

Raymond, Eric S. *The Cathedral and the Bazaar, Rev. Ed.*. Cambridge, MA: O'Reilly, 2001.

Raymond, Eric Steven. "Homesteading the Noosphere." *First Monday* vol. 3, no. 10, 1998.

Raymond, Michael A. "COP: Fusing Battalion Intelligence." *Fires Bulletin*, January-February 2008: 29.

Redmond, Kent C., and Thomas M. Smith. *From Whirlwind to MITRE: the R&D Story of the SAGE Air Defense Computer*. Cambridge, MA: MIT Press, 2000.

Reid-Daly, Ron. *Pamwe Chete: The Legend of the Selous Scouts*. Weltevreden, South Africa: Covo-Day, 2001.

Richelson, Jeffrey T. "MASINT: The New Kid in Town." *International Journal of Intelligence and Counterintelligence* vol. 14, no. 2, 2001: 149-192.

Richelson, Jeffrey T. *America's Space Sentinels: DSP Satellites and National Security*. Lawrence, KS: Kansas University Press, 2001.

Ricks, Thomas E. "Flaws Cited in Effort to Train Iraqi Forces." *Washington Post*, November 21 2006: 1.

Ricks, Thomas E. *The Gamble: General David Petraeus and the American Military Adventure in Iraq, 2006-2008*. New York: Penguin Press, 2009.

Ricks, Thomas. "Situation Called Dire in West Iraq: Anbar is Lost Politically, Marine Analyst Says." *Washington Post*, 11 September 2006.

Roberts, J.M., and T. Sanders. "Before, During and After: Realism, Reflexivity and Ethnography." *The Sociological Review* vol. 53, no. 2, 2005: 294-313.

Rochlin, Gene I. *Trapped in the Net: The Unanticipated Consequences of Computerization*. Princeton, NJ: Princeton

University Press, 1997.

Rodrik, Dani. "How Far Will International Economic Integration Go?" *The Journal of Economic Perspectives* vol. 14, no. 1, 2000: 177-186.

Roland, Alex. "Technology, Ground Warfare, and Strategy: The Paradox of American Experience." *The Journal of Military History* vol. 55, no. 4, 1991: 447-468.

Roland, Alex. *The Military-Industrial Complex*. American Historical Association, 2001.

Roland, Alex. *The Technological Fix: Weapons and the Cost of War*. Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 1995.

Roller, Joseph D. *Leaders Wanted: SOF and CF Integration*. Maxwell Air Force Base, AL: Air Command and Staff College, 2006.

Rorty, Richard. *Philosophy and the Mirror of Nature*. Princeton, NJ: Princeton University Press, 1979.

Rosen, Stephen Peter. *Winning the Next War: Innovation and the Modern Military*. Ithaca, NY: Cornell University Press, 1991.

Rostow, Walter W. "The Beginnings of Air Targeting." *Studies in Intelligence* vol. 7, no. 1, 1963: A1-A24.

Rothstein, Hy S. *Afghanistan and the Troubled Future of Unconventional Warfare*. Annapolis, MD: Naval Institute Press, 2006.

Rovner, Joshua R. *Fixing the Facts: National Security and the Politics of Intelligence*. Ithaca NY: Cornell University Press, 9999.

Rovner, Joshua, and Austin Long. "The Perils of Shallow Theory: Intelligence Reform and the 9/11 Commission." *International Journal of Intelligence and Counterintelligence* vol. 18, no. 4, 2005: 609-637.

Rumsfeld, Donald H. "Transforming the Military." *Foreign Affairs* vol. 81, no. 3, 2002.

Russell, James A. "Innovation in War: Counterinsurgency Operations in Anbar and Ninewa Provinces, Iraq, 2005-2007." *Journal of Strategic Studies* vol. 33, no. 4, 2010: 595 - 624.

Ruttan, Vernon W. *Technology, Growth, and Development: an Induced Innovation Perspective*. Oxford University Press, 2001.

Ryle, Gilbert. "Improvisation." *Mind* vol. 85, no. 3, 1976: 69-83.

Sageman, Marc. *Understanding Terror Networks*. Philadelphia, PA: University of Pennsylvania Press, 2004.

Sapolsky, Harvey M. "On the Theory of Military Innovation." *Breakthroughs* vol. 9, no. 1, 2000: 35-39.

Sapolsky, Harvey M. *Science and the Navy: the History of the Office of Naval Research*. Princeton, NJ: Princeton University Press, 1990.

Sapolsky, Harvey M. *The Polaris System Development: Bureaucratic and Programmatic Success in Government*. Cambridge, MA: Harvard University Press, 1972.

Sapolsky, Harvey M., Benjamin H. Friedman, and Brendan Rittenhouse Green (Eds.). *US Military Innovation After the Cold War: Creation Without Destruction*. New York, NY: Routledge, 2009.

Sapolsky, Harvey M., Eugene Gholz, and Caitlin Talmadge. *US Defense Politics: The Origins of Security Policy*. New York, NY: Routledge, 2008.

Sartre, Jean-Paul. *Being and Nothingness*. New York: Philosophical Library, 1956.

Schlieffen, Alfred Von. "Der Krieg in Der Gegenwart." *Deutsche Revue* vol. 34, no. 1, 1908: 13-24.

Schmitt, Eric. "In a Fatal Error, C.I.A. Picked a Bombing Target Only Once: The Chinese Embassy." *New York Times*, 23 July 1999.

Schultze, Ulrike. "A Confessional Account of an Ethnography about Knowledge Work." *MIS Quarterly* vol. 24, no. 1, 2000: 3-41.

Schultzea, U., and R.J. Boland. "Knowledge Management Technology and the Reproduction of Knowledge Work Practices." *Journal of Strategic Information Systems* vol. 9, 2000: 193-212.

Schwartz, Moshe. "Department of Defense Contractors in Iraq and Afghanistan: Background and Analysis." *Congressional Research Service Report*, 2 July 2010.

Schwarz, Heinrich Joachim. *Techno-Territories: The Spatial, Technological and Social Reorganization of Office Work*. Ph.D. Dissertation, Massachusetts Institute of Technology, Program in Science, Technology and Society, 2003.

Scott, James C. *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*. New Haven, CT: Yale University Press, 1998.

Scott, James C. *The Art of Not Being Governed: An Anarchist History of Upland Southeast Asia*. New Haven, CT: Yale University Press, 2009.

Scott, James C. *Weapons of the Weak: Everyday Forms of Peasant Resistance*. Yale University Press, 1987.

Scott, W. Richard. "Institutional Carriers: Reviewing Modes of Transporting Ideas over Time and Space and Considering Their Consequences." *Industrial and Corporate Change* vol. 12, no. 4, 2003: 879-894.

Scott-Donelan, David. *Tactical Tracking Operations*. Boulder, CO: Paladin Press, 1998.

Searle, Thomas R. "Tribal Engagement in Anbar Province: The Critical Role of Special Operations Forces." *Joint Forces Quarterly*, no. 50, 2008: 62-66.

Seely-Brown, John, and Paul Duguid. *The Social Life of Information*. Cambridge, MA: Harvard Business School Press, 2000.

Sellen, Abigail J., and Richard H. R. Harper. *The Myth of the Paperless Office*. Cambridge, MA: MIT Press, 2003.

Sellin, Lawrence. "Outside View: PowerPoints 'R' Us." *United Press International*, 24 August 2010.

Selznick, Philip. *The Organizational Weapon: A Study of Bolshevik Strategy and Tactics*. Santa Monica, CA: RAND, 1952.

Selznick, Phillip. *Leadership in Administration: A Sociological Interpretation*. Evanston, IL: Row, Peterson and Co, 1957.

Shachtman, Noah. "How Technology Almost Lost the War: In Iraq, the Critical Networks Are Social—Not Electronic." *Wired*, 27 November 2007.

Shachtman, Noah. "Under Worm Assault, Military Bans Disks, USB Drives." *Wired*, 18 November 2008.

Shadid, Anthony. "Iraq Election Highlights Ascendancy of Tribes." *Washington Post*, 25 January 2009: A1.

Shaker, Steven M., and Alan R. Wise. *War Without Men: Robots on the Future Battlefield*. Washington, DC: Pergamon-Brassey's, 1988.

Shannon, Claude E., and Warren Weaver. *The Mathematical Theory of Communication*. Urbana: University of Illinois Press, 1949.

Shanker, Thom, and Matt Richtel. "In New Military, Data Overload Can Be Deadly." *New York Times*, 16 January 2011.

Shapin, Steven. "Here and Everywhere: Sociology of Scientific Knowledge." *Annual Review of Sociology* vol. 21, 1995: 289-32.

Shapiro, Jeremy. "Information and War: Is it a Revolution?." In *Strategic Appraisal: the Changing Role of Information in Warfare*, edited by Zalmay Khalilzad, 113-153. Santa Monica, CA: RAND Corporation, 1999.

Sheffield, Gary, and Dan Todman (Eds.). *Command and Control on the Western Front: The British Army's Experience 1914-18*. Spellmount Publishers, 2004.

Shepsle, Kenneth A. "Studying Institutions: Some Lessons from the Rational Choice Approach." *Journal of Theoretical Politics* vol. 1, no. 2, 1989: 131-147.

Simms, Jennifer E. "A Theory of Intelligence and International Politics." In *National Intelligence Systems: Current Research and Future Prospects*, edited by Gregory F. Treverton and Wilhelm Agrell, 58-92. New York, NY: Cambridge University Press, 2009.

Simon, Herbert A. "Applying Information Technology to Organization Design." *Public Administration Review* vol. 33, no. 3, 1973: 268-278.

Simon, Herbert A. *Administrative Behavior, 4th Edition*. New York: Free Press, 1997.

Singer, P. W. *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. New York, NY: Penguin Press, 2009.

Smith, Brian Cantwell. *On the Origin of Objects*. Cambridge, MA: MIT Press, 1996.

Smith, Edward A. *Effects Based Operations*. Washington D.C.: CCRP Publications Series, 2003.

Smith, Malcolm. *British Air Strategy Between the Wars*. New York, NY: Oxford University Press, 1984.

Smith, Merritt Roe (Ed.). *Military Enterprise and Technological Change: Perspectives on the American Experience*. Cambridge, MA: MIT Press, 1985.

Smith, Merritt Roe, and Leo Marx (Eds.). *Does Technology Drive History? The Dilemma of Technological Determinism*. Cambridge, MA: MIT Press, 1994.

Smith, Niel, and Sean MacFarland. "Anbar Awakens: The Tipping Point." *Military Review*, March-April 2008.

Smith, Rupert. *The Utility of Force: The Art of War in the Modern World*. New York, NY: Penguin Books, 2006.

Smith, Thomas W. "The New Law of War: Legitimizing Hi-Tech and Infrastructural Violence." *International Studies Quarterly* vol. 46, 2002: 355-374.

Snook, Scott. *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks over Northern Iraq*. Princeton: Princeton University Press, 2000.

Snow, C. P. *Science and Government*. Cambridge, MA: Harvard University Press, 1961.

Snyder, Jack L. *The Ideology of the Offensive: Military Decision Making and the Disasters of 1914*. Ithaca, NY: Cornell University Press, 1989.

Sokolowski, Robert. *Introduction to Phenomenology*. Cambridge University Press, 1999.

Spinardi, Graham. *From Polaris to Trident: The Development of US Fleet Ballistic Missile Technology*. Cambridge University Press, 1994.

Spolsky, Joel. "The Law of Leaky Abstractions." *Joel on Software Blog*, 2002. http://www.joelonsoftware.com/articles/LeakyAbstractions.html.

Stanhope-Palmer, Robert. *Tank Trap 1940, or No Battle in Britain*. N. Devon, U.K.: Arthur Stockwell, 1976.

Staniland, Paul. *Explaining Cohesion, Fragmentation, and Control in Insurgent Groups*. Ph.D. Dissertation, Massachusetts Institute of Technology, 2010.

Stanley, Elizabeth A. *Evolutionary Technology in the Current Revolution in Military Affairs: The Army Tactical Command and Control System*. Carlisle, PA: Strategic Studies Institute of the US Army War College, 1998.

Star, Susan Leigh. "The Ethnography of Infrastructure." *American Behavioral Scientist* vol. 43, no. 3, 1999: 377-391.

Steinbruner, John D. *The Cybernetic Theory of Decision: New Dimensions of Political Analysis*. Princeton, NJ: Princeton University Press, 1974.

Sterelny, Kim. "Externalism, Epistemic Artefacts and the Extended Mind." In *The Externalist Challenge*, edited by Richard Schantz, 239-254. Berlin: Walter De Gruyter, 2004.

Sterelny, Kim. *Thought in a Hostile World: The Evolution of Human Cognition*. Malden, MA: Blackwell, 2003.

Stiglitz, Joseph E. "Information and the Change in the Paradigm in Economics." *The American Economic Review* vol. 92, no. 3, 2002: 460-501.

Stiglitz, Joseph E. "The Private Uses of Public Interests: Incentives and Institutions." *Journal of Economic Perspectives* vol. 12, no. 2, 1998: 3-22.

Strassmann, Paul A. "Information Dominance Bows to Network Limitations." *Signal Magazine*, Aug 2010.

Suchman, Lucy A. "Representing Practice in Cognitive Science." In *Representation in Scientific Practice*, edited by Michael Lynch and Steve Woolgar, 301-322. Cambridge, MA: MIT Press, 1990.

Suchman, Lucy A. *Human-Machine Reconfigurations: Plans and Situated Actions, Revised Edition*. New York: Cambridge University Press, 2006.

Sullivan, Gordon R., and Anthony M. Coroalles. *The Army in the Information Age*. Carlisle Barracks, PA: Strategic Studies Institute, 1995.

Sumida, Jon Tetsuro. *Decoding Clausewitz: A New Approach to On War*. Lawrence, KS: Kansas University Press, 2008.

Sunderland, Riley. *Antiguerrilla Intelligence in Malaya, 1948-1960*. Santa Monica, CA: RAND, 1964.

Sweeney, Michael M. "Blue Force Tracking: Building a Joint Capability." In *Information As Power, Volume 3*, edited by Jeffrey L. Caton, Blane R. Clark, Jeffrey L. Groh and Dennis M. Murphy, 107-126. Carlisle Barracks, PA: United States Army War College, 2009.

Taber, Robert. *War of the Flea: The Classic Study of Guerrilla Warfare*. Washington, DC: Potomac Books, 2002.

Talbot, David. "We Got Nothing Until They Slammed Into Us." *Technology Review*, Nov 2004: 107-115.

Tapscott, Don, and Anthony D. Williams. *Wikinomics: How Mass Collaboration Changes Everything*. New York, NY: Penguin Books, 2006.

Tavernise, Sabrina. "Mix of Trust and Despair Helped Turn Tide in Iraq." *New York Times*, 23 October 2010.

Tenet, George. "DCI Statement on the Belgrade Chinese Embassy Bombing." House Permanent Select Committee on Intelligence Open Hearing, 22 July 1999.

Thomas Harding. "Terrorists 'Use Google Maps to Hit UK Troops." *Telegraph*, 13 January 2007.

Thomke, Stefan, and Eric Von Hippel. "Customers As Innovators: A New Way to Create Value." *Harvard Business Review* vol. 80, no. 4, 2002: 74-81.

Thompson, Clive. "Open-Source Spying." *New York Times Magazine*, 3 December 2006.

Thompson, Roger. "Brown Shoes, Black Shoes, and Felt Slippers: Parochialism and the Evolution of the Post-War U.S. Navy." *U.S. Naval War College Center for Naval Warfare Studies Occassional Paper*, 1995.

Tirpak, John A. "Find, Fix, Track, Target, Engage, Assess." *Air Force Magazine* vol. 83, no. 7, 2000.

Todd, Lin. *Iraq Tribal Study–al-Anbar Governorate: The Albu Fahd Tribe, the Albu Mahal Tribe and the Albu Issa Tribe*. Global Resources Group, under contract with the Department of Defense, 2006.

Todman, Dan. "The Grand Lamasery Revisited: General Headquarters on the Western Front, 1914-1918." In *Command and Control on the Western Front: The British Army's Experience 1914-18*, edited by Gary Sheffield and Dan Todman, 39-70. Spellmount Publishers, 2004.

Toffler, Alvin, and Heidi Toffler. *War and Anti-War: Survival At the Dawn of the 21st Century*. Boston, MA: Little, Brown and Co, 1993.

Toliver, Raymond T. *The Interrogator: The Story of Hanns Joachim Scharff, Master Interrogator of the Luftwaffe*. Atglen, PA: Schiffer Publishing, 1997.

Tomasello, Michael. *The Cultural Origins of Human Cognition*. Cambridge, MA: Harvard University Press, 2000.

Tremlett, Giles. "GPS Directs Driver to Death in Spain's Largest Reservoir." *Guardian*, 4 October 2010.

Treverton, Gregory F. *Reshaping National Intelligence in an Age of Information*. New York, NY: Cambridge University Press, 2001.

Trinquier, Roger. *Modern Warfare: A French View of Counterinsurgency*. London: Praeger Security International, 2006.

Trulock, Notra, Kerry Hines, and Anne Herr. "Soviet Military Thought in Transition: Implications for the Long-Term Military Competition." *Pacific-Siera Research Corporation Report*, no. 1831, 1988.

Tuchman, Barbara W. *The Guns of August*. New York, NY: Macmillan, 1994.

Tucker, David, and Christopher J. Lamb. *United States Special Operations Forces*. New York, NY: Columbia University Press, 2007.

Tufte, Edward R. *The Cognitive Style of Power Point*. Cheshire, Connecticut: Graphics Press, 2003.

Tufte, Edward R. *The Visual Display of Quantitative Information*. Cheshire, Connecticut: Graphics Press, 1992.

Turnley, Jessica Glicken. "Retaining a Precarious Value As Special Operations Go Mainstream." *Joint Special Operations University Report*, 08-2 2008.

Tushman, Michael L., and Thomas J. Scanlan. "Boundary Spanning Individuals: Their Role in Information Transfer and Their Antecedents." *The Academy of Management Journal* vol. 24, no. 2, 1981: 289-305.

U.S. Army. *FM 3-24: Counterinsurgency*. Washington DC: U.S. Government Printing Office, 2006.

U.S. Government Accountability Office. "Stronger Management Practices Are Needed to Improve DOD's Software-

Intensive Weapon Acquisitions." *GAO-04-393*, March 2004.

U.S. Joint Chiefs of Staff. *Capstone Concept for Joint Operations*. Washington D.C.: U.S. Government Printing Office, 2009.

U.S. Joint Chiefs of Staff. *Joint Publication 2-0: Doctrine for Intelligence Support to Joint Operations*. Washington D.C.: U.S. Government Printing Office, 2000.

U.S. Joint Chiefs of Staff. *Joint Publication 3-13.1: Joint Doctrine for Command and Control Warfare*. Washington DC: Government Printing Office, 1996.

U.S. Joint Chiefs of Staff. *Joint Publication 3-13: Information Operations*. Washington, DC: Government Printing Office, 2006.

U.S. Joint Chiefs of Staff. *Joint Publication 3-60: Joint Doctrine for Targeting*. Washington DC: Government Printing Office, 2002.

U.S. Joint Chiefs of Staff. *Joint Vision 2010*. U.S. Government Printing Office, 1996.

U.S. Joint Chiefs of Staff. *Joint Vision 2020*. U.S. Government Printing Office, 2000.

U.S. Special Operations Command. *USSOCOM Publication 3-33: Conventional Force and Special Operations Forces Integration and Interoperability Handbook and Checklist, Version 2*. Macdill Air Force Base, FL: USSOCOM, 2006.

Van Atta, Richard H., Michael J. Lippitz, Jasper C. Lupo, Rob Mahoney, and Jack H. Nunn. "Transformation and Transition: DARPA's Role in Fostering an Emerging Revolution in Military Affairs, Volume 1: Overall Assessment." *Institute For Defense Analyses Paper*, P-3698 2003.

Van Creveld, Martin. *Command in War*. Cambridge, MA: Harvard University Press, 1985.

Van Creveld, Martin. *Fighting Power: German and U.S. Army Performance, 1939-1945*. Greenwood Press, 1982.

Van Creveld, Martin. *The Transformation of War*. New York, NY: Free Press, 1991.

Van Evera, Stephen W. "Why States Believe Foolish Ideas: Non-Self-Evaluation By States And Societies." *MIT SSP Working Paper*, 2002. http://web.mit.edu/polisci/research/vanevera/why_states_believe_foolish_ideas.pdf.

Van Evera, Stephen W. *Causes of War: Power and the Roots of Conflict*. Ithaca NY: Cornell University Press, 1999.

Van Evera, Stephen W. *Guide to Methods For Students of Political Science*. Ithaca, NY: Cornell University Press, 1997.

Van Maanen, John. "The Fact of Fiction in Organizational Ethnography." *Administrative Science Quarterly* vol. 24, no. 4, 1979: 539-550.

Van Maanen, John. *Tales of the Field: On Writing Ethnography*. Chicago, IL: University of Chicago Press, 1988.

Varela, Francisco J., Evan Thompson, and Eleanor Rosch. *The Embodied Mind: Cognitive Science and Human Experience*. Cambridge, MA: MIT Press, 1991.

Vaughan, Diane. *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*. Chicago, IL: University of Chicago Press, 1997.

Vego, Milan N. "Operational Command and Control in the Information Age." *Joint Forces Quarterly* vol. 35, 2003: 100-107.

Vego, Milan N. *Joint Operational Warfare: Theory and Practice*. Newport, RI: Naval War College, 2007.

Vest, Jason. "The Dubious Genius of Andrew Marshall." *American Prospect*, February 15 2001.

Vetere, Guido, and Maurizio Lenzerini. "Models For Semantic Interoperability in Service-Oriented Architectures." *IBM Systems Journal* vol. 44, no. 4, 2005: 887-904.

Viegas, Fernanda B., Martin Wattenberg, Jesse Kriss, and Frank Van Ham. "Talk Before You Type: Coordination in Wikipedia." *Hawaii International Conference on System Sciences*, 2007.

Von Hippel, Eric. ""Sticky Information" and the Locus of Problem Solving: Implications for Innovation." *Management Science* vol. 40, no. 4, 1994: 429-439.

Von Hippel, Eric. *Democratizing Innovation*. Cambridge, MA: MIT Press, 2005.

Von Hippel, Eric. *The Sources of Innovation*. New York, NY: Oxford University Press, 1988.

Wallace, Robert, H. Keith Melton, and Henry R. Schlesinger. *Spycraft: The Secret History of the CIA's Spytechs from Communism to Al-Qaeda*. New York, NY: Dutton, 2008.

Walsh, James P., and Gerardo Rivera Ungson. "Organizational Memory." *The Academy of Management Review* vol. 16, no. 1, 1991: 57-91.

Waltz, Kenneth N. *Man, the State, and War*. New York, NY: Columbia University Press, 1954.

Waltz, Kenneth N. *Theory of International Politics*. Boston, MA: McGraw-Hill, 1979.

Watson, Paul. "U.S. Military Secrets for Sale At Afghan Bazaar." *Los Angeles Times*, 10 April 2006.

Watts, Barry D. "Clausewitzian Friction and Future War, Revised Ed." *National Defense University, McNair Paper*, no. 68, 2004.

Watts, Barry D. "Unreported History and Unit Effectiveness." *The Journal of Strategic Studies* vol. 12, no. 1, 1989: 88-98.

Watts, Barry D. *Six Decades of Guided Munitions and Battle Networks: Progress and Prospects*. Washington, DC: Center for Strategic and Budgetary Assessments, 2007.

Watts, Duncan J. "The "New" Science of Networks." *Annual Review of Sociology* vol. 30, 2004: 243-270.

Weber, Max. *From Max Weber: Essays in Sociology*. New York, NY: Oxford University Press, 1946.

Weick, Karl E. *The Social Psychology of Organizing*. Reading, MA: Addison-Wesley Pub, 1979.

Weick, Karl E., and Karlene H. Roberts. "Collective Mind in Organizations: Heedful Interrelating on Flight Decks." *Administrative Science Quarterly* vol. 38, no. 3, 1993: 357-81.

Weigley, Russell F. *The American Way of War: A History of United States Military Strategy and Policy*. Bloomington, IN: Indiana University Press, 1973.

Weiner, Norbert. *Cybernetics or Control and Communication in the Animal and the Machine*. Cambridge, MA: MIT Press, 1965.

West, Bing. *The Strongest Tribe: War, Politics, and the Endgame in Iraq*. New York: Random House, 2008.

Wilford, John Noble. *The Mapmakers, Rev. Ed.*. New York, NY: Vintage Books, 2000.

Wilkinson, Spencer. *The Brain of an Army; The Command of the Sea; The Brain of the Navy.*. London, UK: Gregg Revivals, 1992.

Williamson, Oliver E. "The Economics of Organization: The Transactions Cost Approach." *American Journal of Sociology* vol. 87, no. 3, 1981: 548-77.

Williamson, Oliver E. *The Mechanisms of Governance*. New York: Oxford University Press, 1996.

Wilson, James Q. "Innovation in Organization: Notes Towards a Theory." In *Approaches to Organizational Design*, edited by James D. Thompson, 194-218. University of Pittsburgh Press, 1966.

Wilson, Thomas. *Churchill and the Prof*. London, U.K.: Cassell, 1995.

Wimsatt, William C. "Generative Entrenchment and the Developmental Systems Approach to Evolutionary Process." In *Cycles of Contingency: Developmental Systems and Evolution*, edited by Susan Oyama, Paul E. Griffiths and Russell D. Gray, 219-238. Cambridge: MIT Press, 2001.

Winner, Langdon. "Do Artifacts Have Politics?" *Daedalus* vol. 109, no. 1, 1980: 121-136.

Winner, Langdon. *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought*. Cambridge, MA: MIT Press, 1977.

Winograd, Terry, and Fernando Flores. *Understanding Computers and Cognition: A New Foundation for Design*. Reading, MA: Addison-Wesley Publishing Company, Inc, 1986.

Winterbotham, F. W. *The Ultra Secret*. New York, NY: Harper & Row, 1974.

Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision*. Stanford, CA: Stanford University Press, 1962.

Wolters, Timothy S. *Managing a Sea of Information: Shipboard Command and Control in the United States Navy, 1899-1945*. Ph.D. Dissertation, MIT Program in Science, Technology, and Society, 2003.

Wood, Derek, and Derek Dempster. *The Narrow Margin: The Battle of Britain and the Rise of Air Power, 1930-1940*. Washington, DC: Smithsonian Institution Press, 1990.

Woodward, Bob. "Why Did Violence Plummet? It Wasn't Just the Surge." *Washington Post*, 8 Sept 2008: A9.

Woodward, Bob. *Obama's Wars*. New York, NY: Simon & Schuster, 2010.

Woodward, Bob. *The War Within: A Secret White House History 2006-2008*. New York, NY: Simon & Schuster, 2008.

Yates, Joanne, and Wanda J. Orlikowski. "The Powerpoint Presentation and Its Corollaries: How Genres Shape Communicative Action in Organizations." In *The Cultural Turn: Communicative Practices in Workplaces and the Professions*, edited by Mark Zachry and Charlotte Thralls. Amityville, NY: Baywood Publishing, 2006.

Yates, Joanne. *Control Through Communication: The Rise of System in American Management*. Baltimore, MD: Johns Hopkins University Press, 1993.

Yates, Joanne. *Structuring the Information Age: Life Insurance and Technology in the Twentieth Century*. Baltimore, MD: Johns Hopkins University Press, 2005.

Young, Neil. "British Home Air Defence Planning in the 1920s." *Journal of Strategic Studies* vol. 11, no. 4, 1988: 492 - 508.

Zegart, Amy. *Flawed by Design: The Evolution of the CIA, JCS, and NSC*. Stanford, CA: Stanford University Press, 1999.

Zimet, Elihu, and Edward Skoudis. "A Graphical Introduction to the Structural Elements of Cyberspace." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, 91-112. Washington DC: National Defense University Press, 2009.

Zimmerman, David. "Information and the Air Defence Revolution, 1917–40." *Journal of Strategic Studies* vol. 27, no. 2, 2004: 370 – 394.

Zimmerman, David. *Britain's Shield: Radar and the Defeat of the Luftwaffe*. Phoenix Mill, U.K.:Sutton Publishing Ltd, 2001.

Zittrain, Jonathan L. "The Generative Internet." *Harvard Law Review* vol. 119, no. 7, 2006: 1975-2040.

Zuboff, Shoshana. *In the Age of the Smart Machine: The Future of Work and Power*. New York, NY: Basic Books, 1988.